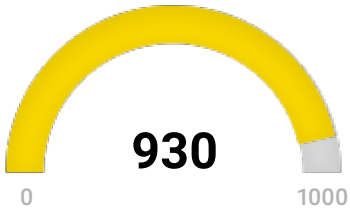
# Good Stuff Manufacturing

Report Date **February 02, 2017**

Report Period **Last 30 Days**

**55** Hosts **2** Externals **1** Sensor




## Top 10 Vulnerabilities*

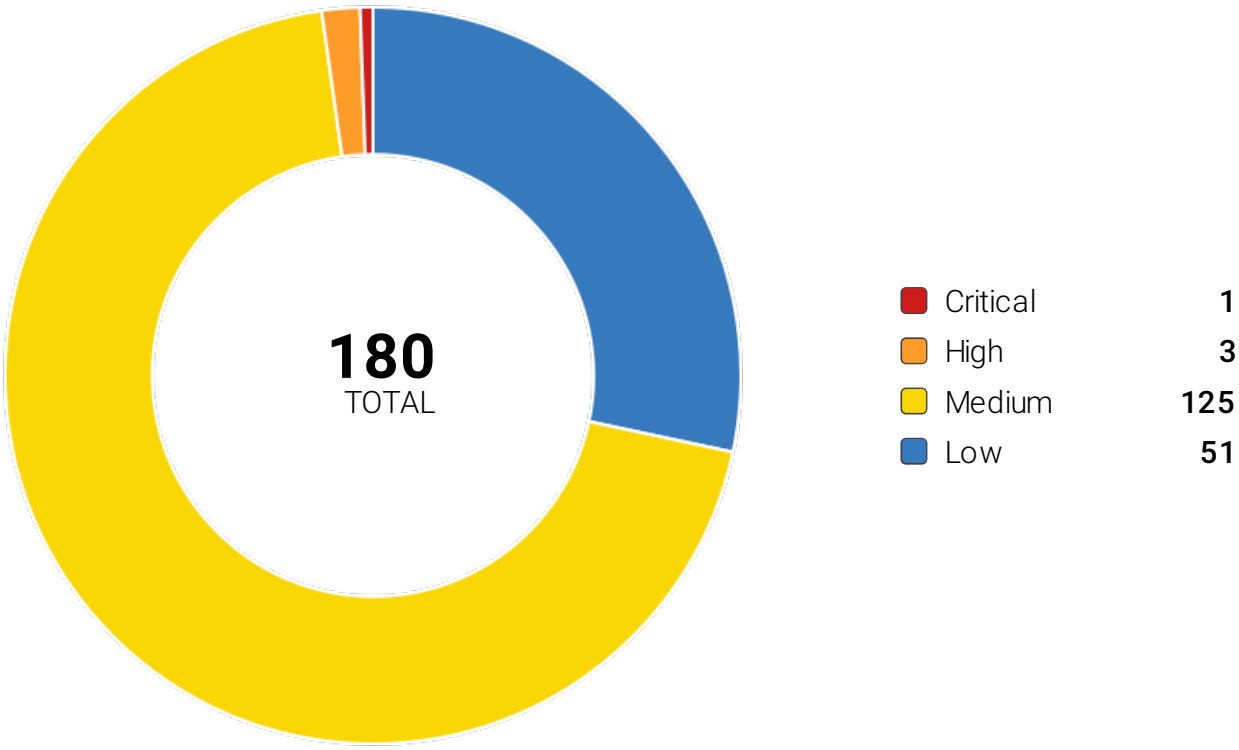
| Vulnerability Name | Severity | Hosts |
|---|---|---|
| VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check) | Critical | 1 |
| VMSA-2015-0001: VMware vCenter Server, ESXi, Workstation, Player, and Fusion upd... | High | 1 |
| VMSA-2014-0008: VMware vSphere product updates to third party libraries (remote c... | High | 1 |
| PHP Use-After-Free Denial Of Service Vulnerability - 02 - Jul15 (Windows) | High | 1 |
| OpenSSL CCS Man in the Middle Security Bypass Vulnerability | Medium | 2 |
| VMSA-2014-0012: VMware vSphere product updates address security vulnerabilities... | Medium | 1 |
| VMSA-2016-0001 VMware ESXi, Fusion, Player, and Workstation updates address imp... | Medium | 1 |
| VMSA-2014-0006: VMware product updates address OpenSSL security vulnerabilitie... | Medium | 1 |
| DCE Services Enumeration | Medium | 19 |
| Check for SSL Weak Ciphers | Medium | 16 |

**Vulnerabilities are sorted descending by severity rating and secondarily by number of hosts affected*

## Most Common Vulnerabilities

| Vulnerability Name | Severity | Hosts |
|---|---|---|
| TCP timestamps | Low | 38 |
| DCE Services Enumeration | Medium | 19 |
| Check for SSL Weak Ciphers | Medium | 16 |
| SSL Certificate Signed Using A Weak Signature Algorithm | Medium | 9 |
| Relative IP Identification number change | Low | 7 |
| SSH Weak MAC Algorithms Supported | Low | 6 |
| Deprecated SSLv2 and SSLv3 Protocol Detection | Medium | 6 |
| POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability | Medium | 6 |
| SSH Weak Encryption Algorithms Supported | Medium | 5 |
| SSL Certification Expired | Medium | 4 |

## Network Vulnerability Profile



## Host Vulnerability Overview

| IP Address | Total Found | Critical | High | Medium | Low | Score |
|---|---|---|---|---|---|---|
| 10.10.0.40 | 19 | 1 | 2 | 15 | 1 | 493 |
| 10.10.0.6 | 16 | 0 | 0 | 15 | 1 | 620 |
| 10.10.0.11 | 11 | 0 | 0 | 10 | 1 | 794 |
| 10.10.0.2 | 10 | 0 | 0 | 8 | 2 | 850 |
| goodstuff.co | 9 | 0 | 0 | 7 | 2 | 868 |
| 10.10.0.200 | 6 | 0 | 0 | 5 | 1 | 920 |
| 10.10.0.4 | 6 | 0 | 0 | 5 | 1 | 921 |
| 10.10.0.134 | 6 | 0 | 0 | 5 | 1 | 921 |
| 10.10.0.176 | 6 | 0 | 0 | 5 | 1 | 921 |
| 10.10.0.155 | 5 | 0 | 1 | 3 | 1 | 924 |
| 10.10.0.21 | 5 | 0 | 0 | 4 | 1 | 937 |
| 10.10.0.179 | 5 | 0 | 0 | 4 | 1 | 939 |
| 10.10.0.253 | 6 | 0 | 0 | 4 | 2 | 940 |
| 10.10.0.12 | 5 | 0 | 0 | 4 | 1 | 941 |
| 10.10.0.132 | 5 | 0 | 0 | 4 | 1 | 941 |
| 10.10.0.181 | 3 | 0 | 0 | 2 | 1 | 972 |
| 10.10.0.202 | 3 | 0 | 0 | 2 | 1 | 972 |
| 10.10.0.206 | 4 | 0 | 0 | 2 | 2 | 972 |
| 10.10.0.210 | 4 | 0 | 0 | 2 | 2 | 972 |
| 10.10.0.213 | 4 | 0 | 0 | 2 | 2 | 972 |
| 10.10.0.214 | 4 | 0 | 0 | 2 | 2 | 972 |
| 10.10.0.216 | 4 | 0 | 0 | 2 | 2 | 972 |
| 10.10.0.182 | 4 | 0 | 0 | 2 | 2 | 972 |
| 10.10.0.194 | 3 | 0 | 0 | 2 | 1 | 973 |
| 10.10.0.209 | 3 | 0 | 0 | 2 | 1 | 973 |
| 10.10.0.190 | 3 | 0 | 0 | 2 | 1 | 974 |
| 10.10.0.3 | 3 | 0 | 0 | 1 | 2 | 983 |
| 10.10.0.5 | 2 | 0 | 0 | 1 | 1 | 985 |
| 10.10.0.203 | 2 | 0 | 0 | 1 | 1 | 986 |
| 10.10.0.204 | 2 | 0 | 0 | 1 | 1 | 986 |
| 10.10.0.205 | 2 | 0 | 0 | 1 | 1 | 986 |
| 10.10.0.117 | 1 | 0 | 0 | 0 | 1 | 996 |
| 10.10.0.193 | 1 | 0 | 0 | 0 | 1 | 996 |

## Host Vulnerability Overview *(Continued)*

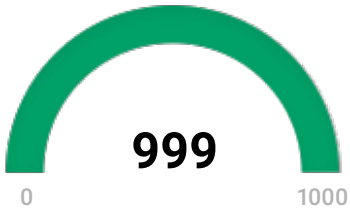
| IP Address | Total Found | Critical | High | Medium | Low | Score |
|---|---|---|---|---|---|---|
| 10.10.0.25 | 1 | 0 | 0 | 0 | 1 | 997 |
| 10.10.0.104 | 2 | 0 | 0 | 0 | 2 | 997 |
| 10.10.0.180 | 1 | 0 | 0 | 0 | 1 | 997 |
| 10.10.0.199 | 1 | 0 | 0 | 0 | 1 | 997 |
| 10.10.0.50 | 1 | 0 | 0 | 0 | 1 | 998 |
| 10.10.0.118 | 0 | 0 | 0 | 0 | 0 | 998 |
| 10.10.0.218 | 1 | 0 | 0 | 0 | 1 | 998 |
| 10.10.0.195 | 1 | 0 | 0 | 0 | 1 | 998 |
| 10.10.0.120 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.121 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.178 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.186 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.188 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.191 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.101 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.20 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.108 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.116 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.111 | 0 | 0 | 0 | 0 | 0 | 999 |
| 10.10.0.113 | 0 | 0 | 0 | 0 | 0 | 999 |
| 66.192.119... | 0 | 0 | 0 | 0 | 0 | 999 |

## Hosts Identified - Not Scanned for Vulnerabilities

| IP Address | MAC Address | MAC Vendor | First Discovered | Duration (Min) |
|---|---|---|---|---|
| 10.10.0.185 | D0:C5:F3:C7:BA:B1 | Apple | 02/02/2017 13:13 | 137 |
| 10.10.0.106 | 90:60:F1:87:E7:E2 | Apple | 02/02/2017 13:45 | 127 |
| 10.10.0.103 | F4:F1:5A:20:7A:8D | Apple | 02/01/2017 22:50 | 46 |

# 66.192.119.134

External Scan

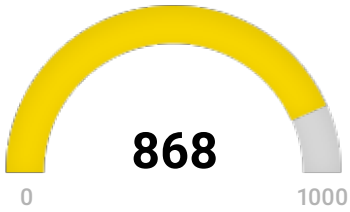



## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# goodstuff.co

External Scan




Medium

## SSH Weak Encryption Algorithms Supported

**Description**

The following weak client-to-server encryption algorithms are supported by the remote service: aes128-cbc aes256-cbc 3des-cbc arcfour128 cast128-cbc arcfour256 blowfish-cbc arcfour rijndael-cbc@lysator.liu.se aes192-cbc The following weak server-to-client encryption algorithms are supported by the remote service: aes128-cbc aes256-cbc 3des-cbc arcfour128 cast128-cbc arcfour256 blowfish-cbc arcfour rijndael-cbc@lysator.liu.se aes192-cbc

**Solution**

Disable the weak encryption algorithms.

**Port**

22/tcp

**More Information**

https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Medium

## Check for SSL Weak Ciphers

**Description**

Weak ciphers offered by this service: TLS1_0_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**Port**

8443/tcp

Medium

## Check for SSL Weak Ciphers

**Description**

Weak ciphers offered by this service: TLS1_0_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**Port**
995/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_0_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**Port**
993/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_1_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**Port**
465/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_0_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**Port**
443/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_0_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_0_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_1_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**Port**
143/tcp

---


## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1957144614 Paket 2: 1957145902

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---


## SSH Weak MAC Algorithms Supported

**Description**
The following weak client-to-server MAC algorithms are supported by the remote service: hmac-md5-96 hmac-sha1-96 hmac-md5-96-etm@openssh.com hmac-md5 hmac-sha1-96-etm@openssh.com hmac-md5-etm@openssh.com The following weak server-to-client MAC algorithms are supported by the remote service: hmac-md5-96 hmac-sha1-96 hmac-md5-96-etm@openssh.com hmac-md5 hmac-sha1-96-etm@openssh.com hmac-md5-etm@openssh.com

**Solution**
Disable the weak MAC algorithms.

**Port**
22/tcp

---

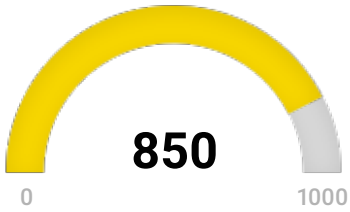
# 10.10.0.2

F8:72:EA:86:BF:BF

MAC Vendor **Cisco Systems**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




---

Medium

## Missing httpOnly Cookie Attribute

**Description**

The cookies: Set-Cookie: webvpn=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure Set-Cookie: webvpnc=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure Set-Cookie: webvpn_portal=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure Set-Cookie: webvpnSharePoint=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure Set-Cookie: webvpnlogin=1; path=/; secure are missing the httpOnly attribute.

**Solution**

Set the 'httpOnly' attribute for any session cookies.

**Port**

8443/tcp

**More Information**

https://www.owasp.org/index.php/HttpOnly
https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

---

Medium

## Check for SSL Weak Ciphers

**Description**

Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA

**Solution**

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**

CVE-2016-2183

**Port**

8443/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**

Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA

**Solution**

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**

CVE-2016-2183

**Port**

443/tcp

Medium

## SSH Weak Encryption Algorithms Supported

**Description**
The following weak client-to-server encryption algorithms are supported by the remote service: aes192-cbc aes128-cbc 3des-cbc aes256-cbc The following weak server-to-client encryption algorithms are supported by the remote service: aes192-cbc aes128-cbc 3des-cbc aes256-cbc

**Solution**
Disable the weak encryption algorithms.

**Port**
22/tcp

**More Information**
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

---

Medium

## SSL Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Description**
Server Temporary Key Size: 1024 bits

**Solution**
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)

**Port**
8443/tcp

**More Information**
https://weakdh.org/

---

Medium

## SSL Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Description**
Server Temporary Key Size: 1024 bits

**Solution**
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)

**Port**
443/tcp

**More Information**
https://weakdh.org/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: 1.2.840.113549.1.9.2=#4947492D4153412E4947492E6C6F63616C,CN=IGI-ASA.igi.local Signature Algorithm: sha1WithRSAEncryption

**Port**

8443/tcp

**More Information**

https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**

The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: 1.2.840.113549.1.9.2=#4947492D4153412E4947492E6C6F63616C,CN=IGI-ASA.igi.local Signature Algorithm: sha1WithRSAEncryption

**Port**

443/tcp

**More Information**

https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 190297187 Paket 2: 190298447

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

http://www.ietf.org/rfc/rfc1323.txt

---

Low

## SSH Weak MAC Algorithms Supported

**Description**

The following weak client-to-server MAC algorithms are supported by the remote service: hmac-sha1-96 hmac-md5 hmac-md5-96 The following weak server-to-client MAC algorithms are supported by the remote service: hmac-sha1-96 hmac-md5 hmac-md5-96

**Solution**

Disable the weak MAC algorithms.

**Port**

22/tcp

---

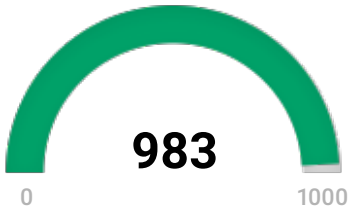
# 10.10.0.3

90:6C:AC:5B:A9:EB

MAC Vendor **Fortinet**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




---

Medium

## Check for SSL Weak Ciphers

**Description**

Weak ciphers offered by this service: TLS1_RSA_DES_64_CBC_SHA TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**

CVE-2016-2183

**Port**

8010/tcp

---

Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 146406378 Paket 2: 146406507

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

http://www.ietf.org/rfc/rfc1323.txt

---

Low

## SSH Weak MAC Algorithms Supported

**Description**

The following weak client-to-server MAC algorithms are supported by the remote service: hmac-sha1-96 The following weak server-to-client MAC algorithms are supported by the remote service: hmac-sha1-96

**Solution**

Disable the weak MAC algorithms.

**Port**

22/tcp

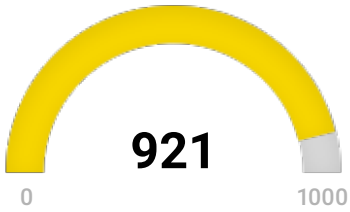
# 10.10.0.4

00:15:5D:00:05:0A

MAC Vendor **Microsoft**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49153] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49153] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49153] Annotation: DHCPv6 Client LRPC Endpoint Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: IdSegSrv service UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: Adh APIs UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49154] Annotation: AppInfo Port: 49155/tcp UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Annotation: Impl friendly name UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Annotation: MS NT Directory DRS Interface UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Named

pipe : lsass Win32 service or process : lsass.exe Description : LSA access UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.4[49155] Annotation: KeyIso Port: 49173/tcp UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_http:10.10.0.4[49173] Annotation: MS NT Directory DRS Interface UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_http:10.10.0.4[49173] Named pipe : lsass Win32 service or process : lsass.exe Description : LSA access UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_http:10.10.0.4[49173] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_http:10.10.0.4[49173] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_http:10.10.0.4[49173] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_http:10.10.0.4[49173] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_http:10.10.0.4[49173] Annotation: KeyIso Port: 49174/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49174] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.4[49174] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.4[49174] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49174] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.4[49174] Annotation: KeyIso Port: 49175/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49175] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49175] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49175] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49175] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49175] Port: 49180/tcp UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_ip_tcp:10.10.0.4[49180] Annotation: 50555 Port: 49205/tcp UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49205] UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[49205] Port: 49229/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.4[49229] Port: 49275/tcp UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:10.10.0.4[49275] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server Port: 53010/tcp UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[53010] Annotation: Frs2 Service Port: 54859/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.4[54859] Annotation: Remote Fw APIs Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---


## Use LDAP search request to retrieve information from NT Directory Services

**Description**
The following information was pulled from the server via a LDAP request: NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=IGI,DC=local

**Solution**
If pre-Windows 2000 compatibility is not required, remove pre-Windows 2000 compatibility as follows : - start cmd.exe - execute the command : net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete - restart the remote host

**Port**

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=DC2.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 26837675 Paket 2: 26837809

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

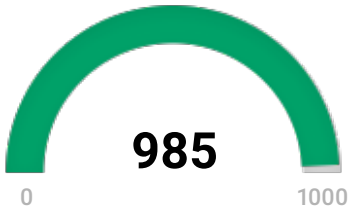
# 10.10.0.5

00:06:F6:90:14:C2

MAC Vendor **Cisco Systems**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## SSH Weak Encryption Algorithms Supported

**Description**

The following weak client-to-server encryption algorithms are supported by the remote service: aes192-cbc aes128-cbc 3des-cbc aes256-cbc The following weak server-to-client encryption algorithms are supported by the remote service: aes192-cbc aes128-cbc 3des-cbc aes256-cbc

**Solution**

Disable the weak encryption algorithms.

**Port**

22/tcp

**More Information**

https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Low

## SSH Weak MAC Algorithms Supported

**Description**

The following weak client-to-server MAC algorithms are supported by the remote service: hmac-sha1-96 hmac-md5 hmac-md5-96 The following weak server-to-client MAC algorithms are supported by the remote service: hmac-sha1-96 hmac-md5 hmac-md5-96

**Solution**

Disable the weak MAC algorithms.

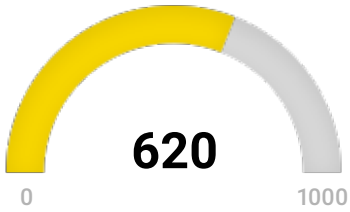
**Port**

22/tcp

# 10.10.0.6

00:15:5D:00:05:0F

MAC Vendor **Microsoft**
Hostname **dc1.igi.local**
First Discovered **02/02/2017 00:06**




Medium DCE Services Enumeration

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

Medium DCE Services Enumeration

**Description**
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49153] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49153] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49153] Annotation: DHCP Client LRPC Endpoint Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: IdSegSrv service UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: Adh APIs UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49154] Port: 49155/tcp UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Annotation: Impl friendly name UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Annotation: MS NT Directory DRS Interface UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : LSA access UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint:

ncacn_ip_tcp:10.10.0.6[49155] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.6[49155] Annotation: KeyIso Port: 49164/tcp UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_http:10.10.0.6[49164] Annotation: MS NT Directory DRS Interface UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_http:10.10.0.6[49164] Named pipe : lsass Win32 service or process : lsass.exe Description : LSA access UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_http:10.10.0.6[49164] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_http:10.10.0.6[49164] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_http:10.10.0.6[49164] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_http:10.10.0.6[49164] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_http:10.10.0.6[49164] Annotation: KeyIso Port: 49165/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49165] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.6[49165] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.6[49165] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49165] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.6[49165] Annotation: KeyIso Port: 49166/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49166] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49166] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49166] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49166] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[49166] Port: 59414/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[59414] Annotation: Remote Fw APIs Port: 59428/tcp UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[59428] Annotation: Frs2 Service Port: 60678/tcp UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[60678] UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1 Endpoint: ncacn_ip_tcp:10.10.0.6[60678] Port: 60690/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.6[60690] Port: 60702/tcp UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:10.10.0.6[60702] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## Use LDAP search request to retrieve information from NT Directory Services

**Description**
The following information was pulled from the server via a LDAP request: NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=IGI,DC=local

**Solution**
If pre-Windows 2000 compatibility is not required, remove pre-Windows 2000 compatibility as follows : - start cmd.exe - execute the command : net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete - restart the remote host

**Port**
389/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA SSL3_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3269/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA SSL3_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
636/tcp

---

Medium

## SSL Certification Expired

**Description**
Expired Certificates: The SSL certificate on the remote service expired on 2015-04-11 23:04:16 Certificate details: subject ...: CN=DC1.IGI.local issued by .: CN=IGI-SVRFP-CA,DC=IGI,DC=local serial ....: 3C000000035EB2C65B98A62F1B000000000003 valid from : 2014-04-11 23:04:16 UTC valid until: 2015-04-11

23:04:16 UTC fingerprint: 5B6169BA9045F818DEB4E27B8BEEF6F15764253C

**Solution**
Replace the SSL certificate by a new one.

**Port**
3269/tcp

---

Medium

## SSL Certification Expired

**Description**
Expired Certificates: The SSL certificate on the remote service expired on 2015-04-11 23:04:16 Certificate details: subject ...: CN=DC1.IGI.local issued by .: CN=IGI-SVRFP-CA,DC=IGI,DC=local serial ....: 3C000000035EB2C65B98A62F1B000000000003 valid from : 2014-04-11 23:04:16 UTC valid until: 2015-04-11 23:04:16 UTC fingerprint: 5B6169BA9045F818DEB4E27B8BEEF6F15764253C The SSL certificate on the remote service expired on 2015-04-11 23:04:16 Certificate details: subject ...: CN=DC1.IGI.local issued by .: CN=IGI-SVRFP-CA,DC=IGI,DC=local serial ....: 3C000000035EB2C65B98A62F1B000000000003 valid from : 2014-04-11 23:04:16 UTC valid until: 2015-04-11 23:04:16 UTC fingerprint: 5B6169BA9045F818DEB4E27B8BEEF6F15764253C

**Solution**
Replace the SSL certificate by a new one.

**Port**
636/tcp

---

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**
Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**
CVE-2014-3566

**Port**
3269/tcp

**More Information**
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**
Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**
CVE-2014-3566

**Port**
636/tcp

**More Information**
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
3269/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

Medium

## Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
636/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=DC1.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject:

CN=DC1.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3269/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=DC1.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
636/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 6002848 Paket 2: 6002973

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

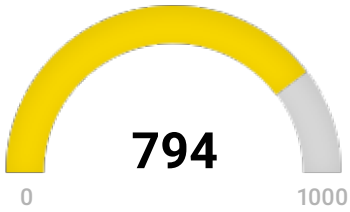
**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.11

00:0C:29:2A:A0:36

MAC Vendor **VMware**
Hostname **svrts1.igi.local**
First Discovered **02/01/2017 22:49**




Medium DCE Services Enumeration

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

Medium DCE Services Enumeration

**Description**
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 3388/tcp UUID: 44e265dd-7daf-42cd-8560-3cdb6e7a2729, version 1 Endpoint: ncacn_http:10.10.0.11[3388] Annotation: TsProxy UUID: 958f92d8-da20-467a-bbe3-65e7e9b4edcf, version 1 Endpoint: ncacn_http:10.10.0.11[3388] Annotation: TsProxyMgmt Port: 5504/tcp UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2 Endpoint: ncacn_ip_tcp:10.10.0.11[5504] Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49152] Port: 49153/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49153] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.11[49153] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.11[49153] Annotation: RemoteAccessCheck UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.11[49153] Annotation: KeyIso Port: 49154/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49154] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49154] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49154] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49154] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49154] Annotation: DHCPv6 Client LRPC Endpoint Port: 49155/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: IKE/Authip API UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: IdSegSrv service UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: Adh APIs UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version

1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: Impl friendly name UUID: 7d814569-35b3-4850-bb32-83035fcebf6e, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49155] Annotation: IAS RPC server Port: 49156/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.11[49156] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.11[49156] Annotation: RemoteAccessCheck UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.11[49156] Annotation: KeyIso Port: 49157/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49157] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49157] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49157] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49157] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49157] Port: 49251/tcp UUID: 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49251] Named pipe : HydraLsPipe Win32 service or process : lserver.exe Description : Terminal Server Licensing UUID: 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49251] Port: 49381/tcp UUID: aa177641-fc9b-41bd-80ff-f964a701596f, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49381] UUID: 32e36e84-4ba2-496c-ba85-fb450f325107, version 2 Endpoint: ncacn_ip_tcp:10.10.0.11[49381] Port: 49384/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.11[49384] Port: 49387/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49387] Annotation: Remote Fw APIs Port: 49389/tcp UUID: 9b3195fe-d603-43d1-a0d5-9072d7cde122, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49389] UUID: 89759fce-5a25-4086-8967-de12f39a60b5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49389] Port: 49456/tcp UUID: 3357951c-a1d1-47db-a278-ab945d063d03, version 1 Endpoint: ncacn_ip_tcp:10.10.0.11[49456] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA SSL3_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers

anymore.

**CVE**
CVE-2016-2183

**Port**
443/tcp

---

Medium

## SSL Certification Expired

**Description**
Expired Certificates: The SSL certificate on the remote service expired on 2014-12-22 19:00:25 Certificate details: subject ....: CN=SvrTS1.IGI.local issued by .: CN=SvrTS1.IGI.local serial ....: 47BA1382EC65ABB941D22F70EA511755 valid from : 2014-06-22 19:00:25 UTC valid until: 2014-12-22 19:00:25 UTC fingerprint: 8A80BB9CD4A7C5EBD6DFEB57F3B4E13A4F45A00E

**Solution**
Replace the SSL certificate by a new one.

**Port**
443/tcp

---

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**
Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**
CVE-2014-3566

**Port**
443/tcp

**More Information**
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
443/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=SvrTS1.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=Default CA,C=US Signature Algorithm: sha1WithRSAEncryption Subject: CN=SVRTS1 Signature Algorithm: sha1WithRSAEncryption

**Port**
2002/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=SvrTS1.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
443/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 26789943 Paket 2: 26790068

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

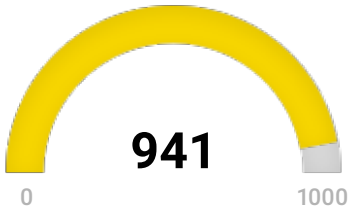
# 10.10.0.12

00:21:9B:9A:0B:32

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 5504/tcp UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2 Endpoint: ncacn_ip_tcp:10.10.0.12[5504] Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49153] Annotation: Wcm Service Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: IP Transition Configuration endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: Adh APIs UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: IdSegSrv service UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: Proxy Manager client server endpoint UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49154] Port: 49155/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.12[49155] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.12[49155] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49167/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49167] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-

942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49167] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49167] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49167] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49167] Port: 49174/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49174] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49183/tcp UUID: aa177641-fc9b-41bd-80ff-f964a701596f, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49183] UUID: 32e36e84-4ba2-496c-ba85-fb450f325107, version 2 Endpoint: ncacn_ip_tcp:10.10.0.12[49183] Port: 49186/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.12[49186] Port: 49189/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49189] Annotation: Remote Fw APIs Port: 49190/tcp UUID: 9b3195fe-d603-43d1-a0d5-9072d7cde122, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49190] UUID: 89759fce-5a25-4086-8967-de12f39a60b5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.12[49190] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=HYPERV3.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 3606665 Paket 2: 3606797

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global

timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

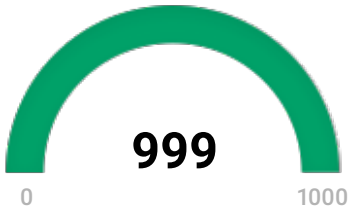
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.20

B4:E9:B0:6B:F1:5E

MAC Vendor **Cisco Systems**
Hostname **N/A**
First Discovered **02/01/2017 22:51**



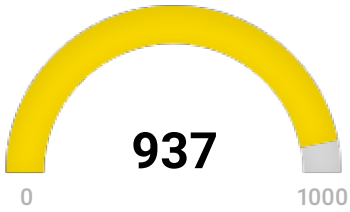

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.21

00:11:32:35:48:4D

MAC Vendor **Synology Incorporated**
Hostname **diskstation.igi.local**
First Discovered **02/01/2017 22:49**




Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS_1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
5102/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS_1_2_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
443/tcp

---

Medium

## Synology DiskStation Manager Cross-Site Scripting Vulnerability

**Description**
Vulnerable url: https://10.10.0.21:5102/webapi/entry.cgi?compound=%5B{"api"%3a"
<img+src%3dx+onload%3dalert(document.cookie)>"%2c"method"%3a"status"%2c"version"%3a1}%2c{"api"%3a"S

**Solution**
Upgrade to the Synology DiskStation Manager 5.2-5565 Update 1 or later, For updates refer to https://www.synology.com/en-global/releaseNote/DS214play

**Port**
5102/tcp

**More Information**
http://packetstormsecurity.com/files/132050/synologydiskstation-xss.txt

https://www.securify.nl/advisory/SFY20150503/reflected_cross_site_scripting_in_synology_diskstation_manage

---

Medium

## Synology DiskStation Manager Cross-Site Scripting Vulnerability

**Description**

Vulnerable url: http://10.10.0.21:5101/webapi/entry.cgi?compound=%5B{"api"%3a"
<img+src%3dx+onload%3dalert(document.cookie)>"%2c"method"%3a"status"%2c"version"%3a1}%2c{"api"%3a"S

**Solution**

Upgrade to the Synology DiskStation Manager 5.2-5565 Update 1 or later, For updates refer to https://www.synology.com/en-global/releaseNote/DS214play

**Port**

5101/tcp

**More Information**

http://packetstormsecurity.com/files/132050/synologydiskstation-xss.txt
https://www.securify.nl/advisory/SFY20150503/reflected_cross_site_scripting_in_synology_diskstation_manage

---

Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 191179608 Paket 2: 191180932

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

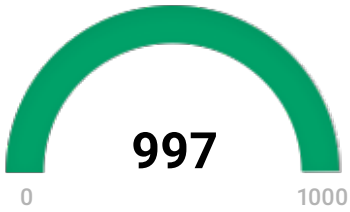
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.25

44:94:FC:35:C7:D8

MAC Vendor **Netgear**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 180721038 Paket 2: 180721305

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

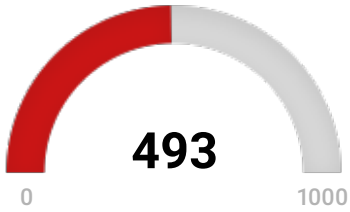
# 10.10.0.40

00:1A:A0:CE:BA:A6

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Critical

## VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check)

**Description**

ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 3021178

**Solution**

Apply the missing patch(es).

**CVE**

CVE-2015-5177
CVE-2015-2342
CVE-2015-1047

**Port**

general/tcp

**More Information**

http://www.vmware.com/security/advisories/VMSA-2015-0007.html

High

## VMSA-2014-0008: VMware vSphere product updates to third party libraries (remote check)

**Description**

ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 2323231

**Solution**

Apply the missing patch(es).

**CVE**

CVE-2014-0114
CVE-2013-4590
CVE-2013-4322
CVE-2014-0050
CVE-2013-0242
CVE-2013-1914

**Port**

general/tcp

**More Information**

http://www.vmware.com/security/advisories/VMSA-2014-0008.html

High

## VMSA-2015-0001: VMware vCenter Server, ESXi, Workstation, Player, and Fusion updates address security issues (remote check)

**Description**

ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 1743201

**Solution**

Apply the missing patch(es).

**CVE**
CVE-2014-8370
CVE-2015-1043
CVE-2015-1044
CVE-2014-3513
CVE-2014-3567
CVE-2014-3566
CVE-2014-3568
CVE-2014-3660

**Port**
general/tcp

**More Information**
http://www.vmware.com/security/advisories/VMSA-2015-0001.html

---

Medium

## VMSA-2014-0006: VMware product updates address OpenSSL security vulnerabilities (remote check)

**Description**
ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 1900470

**Solution**
Apply the missing patch(es).

**CVE**
CVE-2014-0224
CVE-2014-0198
CVE-2010-5298
CVE-2014-3470

**Port**
general/tcp

**More Information**
http://www.vmware.com/security/advisories/VMSA-2014-0006.html

---

Medium

## OpenSSL CCS Man in the Middle Security Bypass Vulnerability

**Solution**
Updates are available.

**CVE**
CVE-2014-0224

**Port**
5989/tcp

**More Information**
http://www.securityfocus.com/bid/67899
http://openssl.org/

---

Medium

## OpenSSL CCS Man in the Middle Security Bypass Vulnerability

**Solution**
Updates are available.

**CVE**
CVE-2014-0224

**Port**
443/tcp

**More Information**
http://www.securityfocus.com/bid/67899
http://openssl.org/

---

Medium

## VMSA-2016-0001 VMware ESXi, Fusion, Player, and Workstation updates address important guest privilege escalation vulnerability (remote check)

**Description**
ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 3021178

**Solution**
Apply the missing patch(es).

**CVE**
CVE-2015-6933

**Port**
general/tcp

**More Information**
http://www.vmware.com/security/advisories/VMSA-2016-0001.html

---

Medium

## VMSA-2014-0012: VMware vSphere product updates address security vulnerabilities (remote check)

**Description**
ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 2323231

**Solution**
Apply the missing patch(es).

**CVE**
CVE-2014-3797
CVE-2014-8371
CVE-2013-2877
CVE-2014-0191
CVE-2014-0015
CVE-2014-0138
CVE-2013-1752
CVE-2013-4238

**Port**
general/tcp

**More Information**
http://www.vmware.com/security/advisories/VMSA-2014-0012.html

---

Medium

## VMSA-2014-0005: VMware Workstation, Player, Fusion, and ESXi patches address a guest privilege escalation

**Description**
ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 1743201

**Solution**
Apply the missing patch(es).

**CVE**
CVE-2014-3793

**Port**

general/tcp

**More Information**

http://www.vmware.com/security/advisories/VMSA-2014-0005.html

---

Medium

## VMSA-2013-0016 VMware ESXi and ESX unauthorized file access through vCenter Server and ESX (remote check)

**Description**

ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 1312874

**Solution**

Apply the missing patch(es).

**CVE**

CVE-2013-5973

**Port**

general/tcp

**More Information**

http://www.vmware.com/security/advisories/VMSA-2013-0016.html

---

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**

Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**

CVE-2014-3566

**Port**

5989/tcp

**More Information**

https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**

Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**

CVE-2014-3566

**Port**

443/tcp

**More Information**

https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## Deprecated SSL v2 and SSL v3 Protocol Detection

Medium Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
5989/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

## Medium Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
443/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

## Medium VMSA-2014-0001 VMware ESXi address several security issues (remote check).

**Description**
ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 1483097

**Solution**
Apply the missing patch(es).

**CVE**
CVE-2014-1207
CVE-2014-1208

**Port**
general/tcp

**More Information**
http://www.vmware.com/security/advisories/VMSA-2014-0001.html

---

## Medium VMSA-2013-0011 VMware ESX and ESXi updates to third party libraries (remote check)

**Description**
ESXi Version: 5.1.0 Detected Build: 1065491 Fixed Build: 1142907

**Solution**

**Solution**
Apply the missing patch(es).

**CVE**
CVE-2013-1661

**Port**
general/tcp

**More Information**
http://www.vmware.com/security/advisories/VMSA-2013-0011.html

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: 1.2.840.113549.1.9.2=#313337313233373432322C353634643737363137323635323034393666536333265, ESX Server Default Certificate,O=VMware\, Inc,L=Palo Alto,ST=California,C=US Signature Algorithm: sha1WithRSAEncryption

**Port**
5989/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: 1.2.840.113549.1.9.2=#313337313233373432322C353634643737363137323635323034393666536333265, ESX Server Default Certificate,O=VMware\, Inc,L=Palo Alto,ST=California,C=US Signature Algorithm: sha1WithRSAEncryption

**Port**
443/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 26957288 Paket 2: 26957427

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

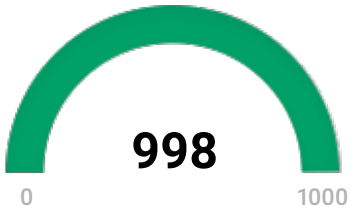
**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.50

04:A1:51:35:32:F4

MAC Vendor **Netgear**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 162528679 Paket 2: 162528804

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

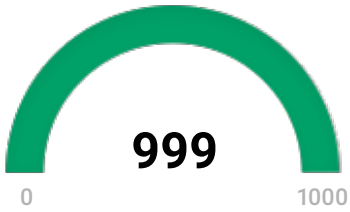
**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.101

34:23:BA:DB:CB:CC

MAC Vendor **Samsung Electro-mechanics(thailand)**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

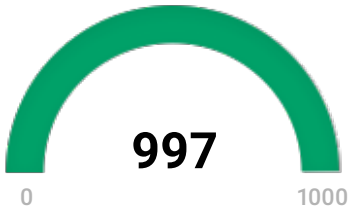
# 10.10.0.104

40:F0:2F:48:D5:36

MAC Vendor **Liteon Technology**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1464956705 Paket 2: 1464957984

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

http://www.ietf.org/rfc/rfc1323.txt

Low

## Relative IP Identification number change

**Solution**

Contact your vendor for a patch

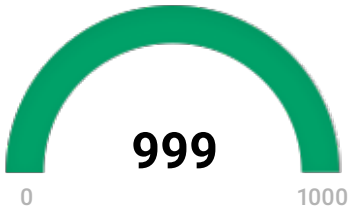
**Port**

general/tcp

# 10.10.0.108

C4:9A:02:8C:B6:31

MAC Vendor **LG Electronics (Mobile Communications)**
Hostname **N/A**
First Discovered **02/02/2017 13:02**



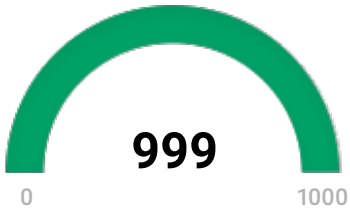

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.111

5C:F7:E6:F3:C6:12

MAC Vendor **Apple**
Hostname **N/A**
First Discovered **02/02/2017 13:43**



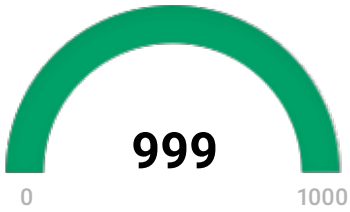

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.113

9C:FC:01:4B:49:41

MAC Vendor **Apple**
Hostname **N/A**
First Discovered **02/02/2017 14:23**



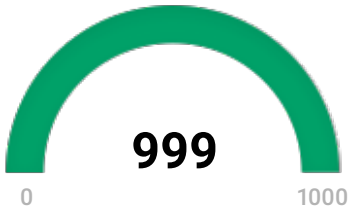

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.116

2C:20:0B:1B:64:C2

MAC Vendor **Apple**
Hostname **N/A**
First Discovered **02/02/2017 13:32**



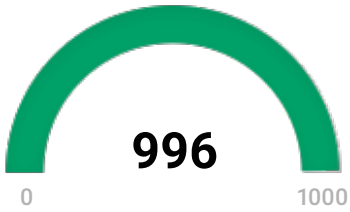

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.117

B4:B6:76:DA:BE:66

MAC Vendor **Intel Corporate**
Hostname **N/A**
First Discovered **02/02/2017 12:49**




Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 148685660 Paket 2: 148686925

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

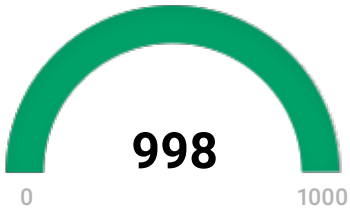
**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.118

B8:27:EB:CB:39:2D

MAC Vendor **Raspberry Pi Foundation**
Hostname **N/A**
First Discovered **02/01/2017 22:49**



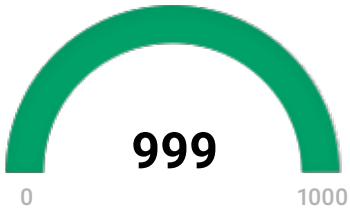

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.120

00:80:91:74:B6:7F

MAC Vendor **Tokyo Electric**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

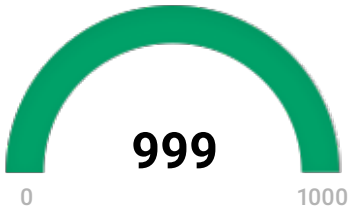
# 10.10.0.121

00:1E:8F:18:E9:FA

MAC Vendor **Canon**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

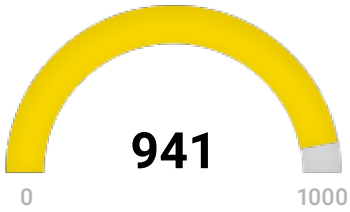
# 10.10.0.132

00:15:5D:00:05:0C

MAC Vendor **Microsoft**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49153] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49153] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49153] Annotation: DHCP Client LRPC Endpoint Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: IdSegSrv service UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: Adh APIs UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: Impl friendly name UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49154] Annotation: AppInfo Port: 49155/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49155] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint:

ncacn_ip_tcp:10.10.0.132[49155] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49155] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49155] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49155] Port: 49156/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.132[49156] Port: 49157/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49157] Annotation: Remote Fw APIs Port: 49158/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.132[49158] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=jump Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 27175899 Paket 2: 27176030

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

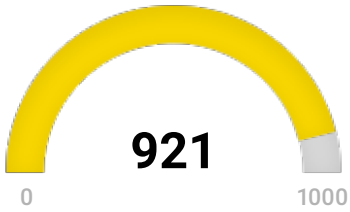
**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.134

00:25:90:DC:96:61

MAC Vendor **Super Micro Computer**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium

## OpenSSL CCS Man in the Middle Security Bypass Vulnerability

**Solution**
Updates are available.
**CVE**
CVE-2014-0224
**Port**
443/tcp
**More Information**
http://www.securityfocus.com/bid/67899
http://openssl.org/

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA SSL3_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5
**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.
**CVE**
CVE-2016-2183
**Port**
443/tcp

Medium

## SSL Certification Expired

**Description**
Expired Certificates: The SSL certificate on the remote service expired on 2016-10-31 00:00:00 Certificate details: subject ...: CN=IPMI,OU=Software,O=Super Micro Computer,ST=California,C=US issued by .: CN=IPMI,OU=Software,O=Super Micro Computer,ST=California,C=US serial ....: 01 valid from : 2013-10-31 00:00:00 UTC valid until: 2016-10-31 00:00:00 UTC fingerprint: 5715C0BB9501EDD61227A9EF9248F1085C7B0268
**Solution**
Replace the SSL certificate by a new one.
**Port**
443/tcp

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**
Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**
CVE-2014-3566

**Port**
443/tcp

**More Information**
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
443/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 717204755 Paket 2: 717204915

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

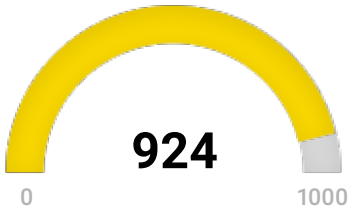
**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.155

C8:1F:66:03:99:CD

MAC Vendor **Dell**
Hostname **licensing.igius.com**
First Discovered **02/01/2017 22:49**




High

## PHP Use-After-Free Denial Of Service Vulnerability - 02 - Jul15 (Windows)

**Description**
Installed Version: 5.5.12 Fixed Version: 5.5.25

**Solution**
Upgrade to PHP 5.5.22 or 5.6.6 or later. For updates refer to http://www.php.net

**CVE**
CVE-2015-1351

**Port**
80/tcp

**More Information**
http://bugzilla.redhat.com/show_bug.cgi?id=1185900
http://openwall.com/lists/oss-security/2015/01/24/9

---

Medium

## Missing httpOnly Cookie Attribute

**Description**
The cookies: Set-Cookie: PHPSESSID=qt9beifc1bp2knsq0a31krn4r7; path=/ are missing the httpOnly attribute.

**Solution**
Set the 'httpOnly' attribute for any session cookies.

**Port**
80/tcp

**More Information**
https://www.owasp.org/index.php/HttpOnly
https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

---

Medium

## DCE Services Enumeration

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## DCE Services Enumeration

**Description**
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49153] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49153] Annotation: Security Center Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49154] Annotation: XactSrv service UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49154] Port: 49159/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49159] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49178/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.155[49178] Port: 49181/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49181] Annotation: Remote Fw APIs UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.155[49181] Annotation: IPSec Policy agent endpoint Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---


## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 19457271 Paket 2: 19457405

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

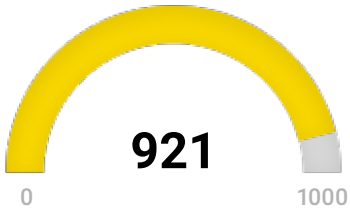
**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.176

C0:3F:D5:6C:36:8B

MAC Vendor **Elitegroup Computer Systems**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA SSL3_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
9390/tcp

Medium

## SSL Certification Expired

**Description**
Expired Certificates: The SSL certificate on the remote service expired on 2016-10-19 19:28:17 Certificate details: subject ...: 1.2.840.113549.1.9.1=#6F70656E766173736440756265726775617264,CN=uberguard,OU=Server certificate for uberguard,O=UberGuard,L=Rochester,ST=NY,C=US issued by .: 1.2.840.113549.1.9.1=#6361407562657267756 17264,CN=uberguard,OU=Certification Authority for uberguard,O=UberGuard,L=Rochester,ST=NY,C=US serial ....: 01 valid from : 2015-10-20 19:28:17 UTC valid until: 2016-10-19 19:28:17 UTC fingerprint: 5600D7945DC431828A6E82C2C4573F71B7D63F41

**Solution**
Replace the SSL certificate by a new one.

**Port**
9390/tcp

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**
Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**
CVE-2014-3566

**Port**

9390/tcp

**More Information**

https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**

9390/tcp

**More Information**

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

Medium

## SSH Weak Encryption Algorithms Supported

**Description**

The following weak client-to-server encryption algorithms are supported by the remote service: aes192-cbc aes256-cbc arcfour128 arcfour aes128-cbc 3des-cbc arcfour256 rijndael-cbc@lysator.liu.se cast128-cbc blowfish-cbc The following weak server-to-client encryption algorithms are supported by the remote service: aes192-cbc aes256-cbc arcfour128 arcfour aes128-cbc 3des-cbc arcfour256 rijndael-cbc@lysator.liu.se cast128-cbc blowfish-cbc

**Solution**

Disable the weak encryption algorithms.

**Port**

22/tcp

**More Information**

https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

---

Low

## SSH Weak MAC Algorithms Supported

**Description**

The following weak client-to-server MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-sha1-96 hmac-md5-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-sha1-96-etm@openssh.com The following weak server-to-client MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-sha1-96 hmac-md5-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-sha1-96-etm@openssh.com

**Solution**

Disable the weak MAC algorithms.

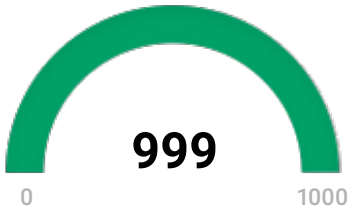
**Port**

22/tcp

# 10.10.0.178

D8:BB:2C:7E:EA:A7

MAC Vendor **Apple**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

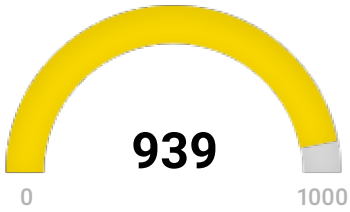
# 10.10.0.179

54:04:A6:DB:F2:A0

MAC Vendor **Asustek Computer**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49152] Port: 49153/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49153] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.179[49153] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.179[49153] Annotation: RemoteAccessCheck Port: 49154/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49154] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49154] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49154] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49154] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49154] Annotation: DHCP Client LRPC Endpoint Port: 49155/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: Adh APIs UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: IdSegSrv service UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1,

version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49155] Annotation: AppInfo Port: 49156/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.179[49156] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.179[49156] Annotation: RemoteAccessCheck Port: 49164/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49164] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49164] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49164] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49164] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49164] Port: 49195/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.179[49195] Port: 49196/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.179[49196] Annotation: Remote Fw APIs Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=Hyperv2.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 14985052 Paket 2: 14985182

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl

-p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

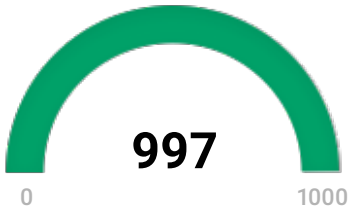
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.180

60:F8:1D:B3:50:84

MAC Vendor **Apple**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1788896690 Paket 2: 1788897822

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

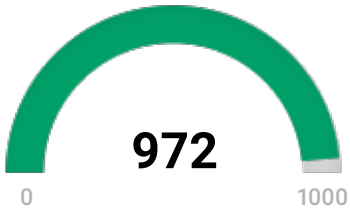
# 10.10.0.181

F4:8E:38:B8:D0:FA

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49664] Port: 49665/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49665] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49665] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49665] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49665] Annotation: Security Center Port: 49666/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: Adh APIs UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: IKE/Authip API UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: ldSegSrv service UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: AppInfo UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: AppInfo UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49666] Annotation: Impl friendly name Port: 49667/tcp UUID: 12345678-1234-abcd-

ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49667] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49667] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49667] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49667] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49667] Port: 49671/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49671] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.181[49671] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49671] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.181[49671] Annotation: Ngc Pop Key Service Port: 49672/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.181[49672] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 82749712 Paket 2: 82751028

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

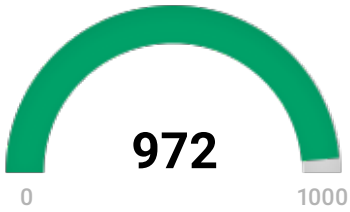
# 10.10.0.182

C4:8E:8F:F8:99:5B

MAC Vendor **Hon Hai Precision Ind.**

Hostname **N/A**

First Discovered **02/02/2017 02:53**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49664] Port: 49665/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: UserMgrCli UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: UserMgrCli UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: Adh APIs UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Annotation: IdSegSrv service UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49665] Port: 49666/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49666] Annotation: Event log TCPIP UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49666] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49666] Annotation: NRP server endpoint Port: 49667/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49667] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49667] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49667] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49667] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49667] Port: 49668/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.182[49668] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.182[49668] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49668] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM

access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.182[49668] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49668] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49668] Annotation: Ngc Pop Key Service Port: 49671/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.182[49671] Port: 49672/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49672] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.182[49672] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49672] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.182[49672] Annotation: Ngc Pop Key Service Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---


## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 67234850 Paket 2: 67236081

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---


## Relative IP Identification number change

**Solution**
Contact your vendor for a patch

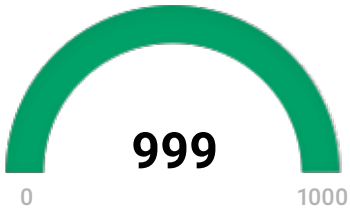
**Port**
general/tcp

---

# 10.10.0.186

B8:27:EB:55:A6:36

MAC Vendor **Raspberry Pi Foundation**
Hostname **N/A**
First Discovered **02/01/2017 22:49**



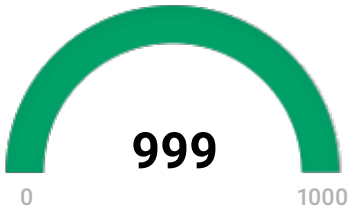

## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

# 10.10.0.188

00:01:36:D3:71:80

MAC Vendor **CyberTAN Technology**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

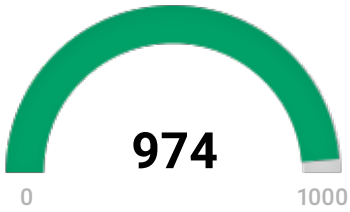
# 10.10.0.190

28:B2:BD:81:46:60

MAC Vendor **Intel Corporate**

Hostname **N/A**

First Discovered **02/02/2017 13:22**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49664] Port: 49665/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49665] Annotation: Event log TCPIP UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49665] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49665] Annotation: NRP server endpoint Port: 49666/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: UserMgrCli UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: UserMgrCli UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: IdSegSrv service UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: AppInfo UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: AppInfo UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] UUID: 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: Vpn APIs UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49666] Annotation: Impl friendly name Port: 49667/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49667] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49667] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49667] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49667] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49667] Port: 49668/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.190[49668] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-

8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.190[49668] Annotation: RemoteAccessCheck UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.190[49668] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49668] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49668] Annotation: Ngc Pop Key Service UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49668] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49685/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.190[49685] Port: 49716/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.190[49716] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---


## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1813999808 Paket 2: 1814001198

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

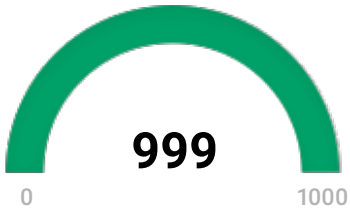
**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.191

B8:27:EB:D4:95:42

MAC Vendor **Raspberry Pi Foundation**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




## No Vulnerabilities Found

This host has no vulnerabilities with a severity rating of Low or above. There may be informational messages available in the Nodeware dashboard.

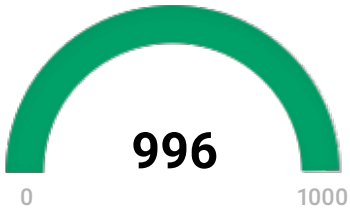
# 10.10.0.193

08:3E:8E:D8:97:25

MAC Vendor **Hon Hai Precision Ind.**

Hostname **N/A**

First Discovered **02/02/2017 13:51**




Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 67524487 Paket 2: 67524617

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

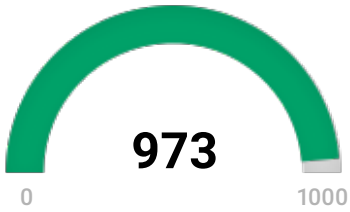
**More Information**

http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.194

B8:EE:65:F2:B5:7B

MAC Vendor **Liteon Technology**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium DCE Services Enumeration

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

Medium DCE Services Enumeration

**Description**
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49664] Port: 49665/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49665] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49665] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49665] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49665] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49665] Annotation: NRP server endpoint Port: 49666/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: UserMgrCli UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: UserMgrCli UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: XactSrv service UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: IKE/Authip API UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: IdSegSrv service UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Annotation: Adh APIs UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49666] Port: 49667/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49667] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49667] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49667] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49667] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49667] Port: 49796/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003,

version 2 Endpoint: ncacn_ip_tcp:10.10.0.194[49796] Port: 49804/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49804] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.194[49804] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49804] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.194[49804] Annotation: Ngc Pop Key Service Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---


## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 182496026 Paket 2: 182497345

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

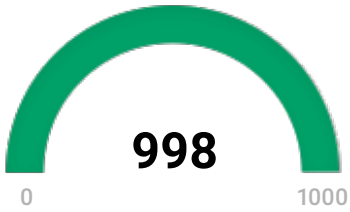
# 10.10.0.195

FC:C2:DE:F9:DC:AE

MAC Vendor **Murata Manufacturing**

Hostname **N/A**

First Discovered **02/02/2017 12:47**




Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 5799486 Paket 2: 5799603

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

http://www.ietf.org/rfc/rfc1323.txt

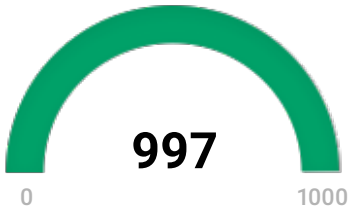
# 10.10.0.199

A4:1F:72:75:92:3E

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 653917677 Paket 2: 653917980

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

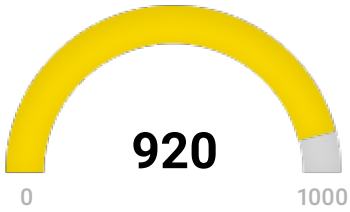
**More Information**

http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.200

00:25:90:DC:98:FD

MAC Vendor **Super Micro Computer**
Hostname **svrfp.igi.local**
First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

Medium

## DCE Services Enumeration

**Description**
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49153] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49153] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49153] Annotation: DHCP Client LRPC Endpoint Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: IdSegSrv service UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: Adh APIs UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: Impl friendly name UUID: 7d814569-35b3-4850-bb32-83035fcebf6e, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: IAS RPC server UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49154] Annotation: AppInfo Port: 49155/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.200[49155] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-

d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.200[49155] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49156/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49156] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49156] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49156] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49156] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49156] Port: 49157/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49157] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49185/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.200[49185] Port: 49186/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:10.10.0.200[49186] Annotation: Remote Fw APIs Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
3389/tcp

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=SvrFP.IGI.local Signature Algorithm: sha1WithRSAEncryption

**Port**
3389/tcp

**More Information**
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Medium

## SSL Certificate Signed Using A Weak Signature Algorithm

**Description**
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=Default CA,C=US Signature Algorithm: sha1WithRSAEncryption Subject: CN=SVRFP Signature Algorithm: sha1WithRSAEncryption

**Port**

2002/tcp

**More Information**

https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

---

Low

## TCP timestamps

**Description**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 27708881 Paket 2: 27709019

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**

general/tcp

**More Information**

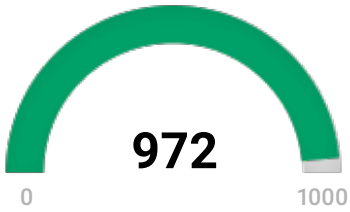
http://www.ietf.org/rfc/rfc1323.txt

---

# 10.10.0.202

08:11:96:1C:97:3C

MAC Vendor **Intel Corporate**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium DCE Services Enumeration

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

Medium DCE Services Enumeration

**Description**
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 2103/tcp UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2103] Annotation: Message Queuing - QMRT V1 UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2103] Annotation: Message Queuing - QMRT V2 UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2103] Annotation: Message Queuing - QM2QM V1 UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2103] Annotation: Message Queuing - RemoteRead V1 Port: 2105/tcp UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2105] Annotation: Message Queuing - QMRT V1 UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2105] Annotation: Message Queuing - QMRT V2 UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2105] Annotation: Message Queuing - QM2QM V1 UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2105] Annotation: Message Queuing - RemoteRead V1 Port: 2107/tcp UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2107] Annotation: Message Queuing - QMRT V1 UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2107] Annotation: Message Queuing - QMRT V2 UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2107] Annotation: Message Queuing - QM2QM V1 UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[2107] Annotation: Message Queuing - RemoteRead V1 Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49664] Port: 49665/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49665] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49665] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49665] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49665] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49665] Annotation: NRP server endpoint Port: 49666/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49666] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.202[49666] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49666] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-

1ac955/a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49666] Annotation: Ngc Pop Key Service Port: 49667/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: UserMgrCli UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: UserMgrCli UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: Adh APIs UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: IdSegSrv service UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: AppInfo UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49667] Annotation: AppInfo Port: 49668/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49668] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49668] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49668] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49668] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49668] Port: 49670/tcp UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49670] Annotation: Message Queuing - QMRT V1 UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49670] Annotation: Message Queuing - QMRT V2 UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49670] Annotation: Message Queuing - QM2QM V1 UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1 Endpoint: ncacn_ip_tcp:10.10.0.202[49670] Annotation: Message Queuing - RemoteRead V1 Port: 49671/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.202[49671] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1618077641 Paket 2: 1618078951

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

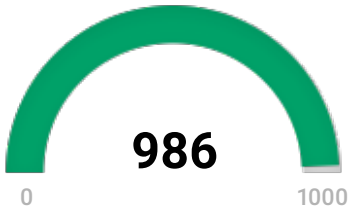
**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.203

B8:27:EB:2E:E8:97

MAC Vendor **Raspberry Pi Foundation**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
9390/tcp

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 26129375 Paket 2: 26129496

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

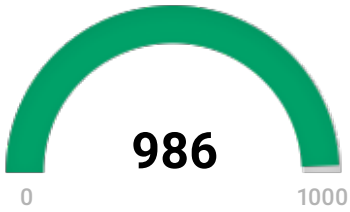
**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.204

B8:27:EB:D0:94:C9

MAC Vendor **Raspberry Pi Foundation**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
9390/tcp

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 26183395 Paket 2: 26183521

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

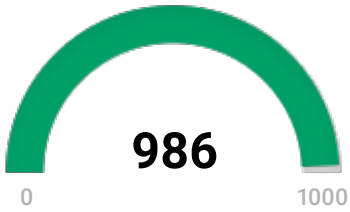
**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

# 10.10.0.205

B8:27:EB:FC:9D:30

MAC Vendor **Raspberry Pi Foundation**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Medium

## Check for SSL Weak Ciphers

**Description**
Weak ciphers offered by this service: TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**
CVE-2016-2183

**Port**
9390/tcp

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 26197222 Paket 2: 26197350

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

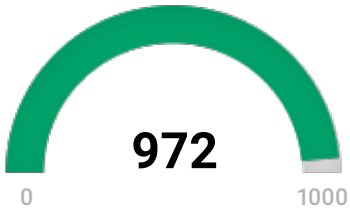
# 10.10.0.206

C8:1F:66:4C:1F:00

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49153] Annotation: Security Center Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49154] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49154] Annotation: XactSrv service Port: 49180/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49180] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49180] Annotation: KeyIso Port: 49228/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.206[49228] Port: 49242/tcp UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49242] Annotation: Spooler function endpoint UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49242] Annotation: Spooler base remote object endpoint UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.206[49242] Annotation: Spooler function endpoint Solution : filter incoming traffic to this port(s).

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 17806771 Paket 2: 17806900

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

Low

## Relative IP Identification number change

**Solution**
Contact your vendor for a patch

**Port**
general/tcp

---

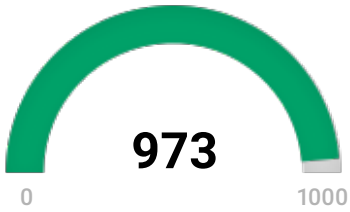
# 10.10.0.209

C8:1F:66:4B:93:18

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49152] Port: 49153/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49153] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49153] Annotation: KeyIso Port: 49154/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49154] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49154] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49154] Annotation: DHCP Client LRPC Endpoint UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49154] Annotation: NRP server endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49154] Annotation: Security Center Port: 49155/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] Annotation: XactSrv service UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.209[49155] Annotation: AppInfo Port: 49260/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.209[49260] Solution : filter incoming traffic to this port(s).

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 6400744 Paket 2: 6400877

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

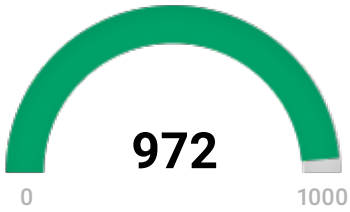
# 10.10.0.210

B8:AC:6F:D7:C7:40

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49153] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49153] Annotation: DHCP Client LRPC Endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49153] Annotation: Wcm Service UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49153] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49153] Annotation: NRP server endpoint Port: 49154/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49154] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.210[49154] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.210[49154] Annotation: RemoteAccessCheck UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.210[49154] Annotation: KeyIso Port: 49155/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: IdSegSrv service UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: Adh APIs UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155]

Annotation: AppInfo UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49155] Annotation: Impl friendly name Port: 49156/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49156] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49156] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49156] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49156] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.210[49156] Port: 49157/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.210[49157] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.210[49157] Annotation: RemoteAccessCheck UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.210[49157] Annotation: KeyIso Port: 49209/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.210[49209] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 74120316 Paket 2: 74120446

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

Low

## Relative IP Identification number change

**Solution**
Contact your vendor for a patch

**Port**
general/tcp

---

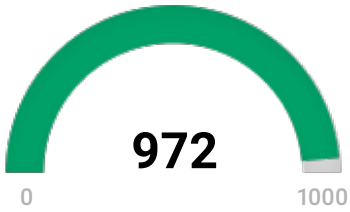
# 10.10.0.213

A4:1F:72:79:D2:3A

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49664] Port: 49665/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: UserMgrCli UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: UserMgrCli UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: Impl friendly name UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: Adh APIs UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: IKE/Authip API UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Annotation: ldSegSrv service UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49665] Port: 49666/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49666] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49666] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49666] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49666] Annotation: Security Center Port: 49668/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49668] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49668] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49668] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49668] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49668] Port: 49673/tcp UUID: 0b1c2170-5732-

4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.213[49673] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.213[49673] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49673] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.213[49673] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49673] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49673] Annotation: Ngc Pop Key Service Port: 49702/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49702] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.213[49702] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49702] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.213[49702] Annotation: Ngc Pop Key Service Port: 49746/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.213[49746] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---


## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 4267255 Paket 2: 4268615

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---


## Relative IP Identification number change

**Solution**
Contact your vendor for a patch

**Port**
general/tcp

---

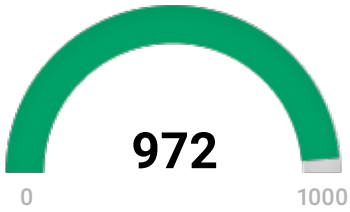
# 10.10.0.214

C8:1F:66:1D:7B:62

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49153] Annotation: Event log TCPIP UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49153] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49153] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49153] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49153] Annotation: NRP server endpoint Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: IdSegSrv service UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: Adh APIs UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: AppInfo UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49154] Annotation: Impl friendly name Port: 49155/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49155] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49155] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint:

ncacn_ip_tcp:10.10.0.214[49155] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49155] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49155] Port: 49157/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.214[49157] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.214[49157] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49157] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.214[49157] Annotation: KeyIso Port: 49173/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.214[49173] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.214[49173] Annotation: KeyIso Port: 58847/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.214[58847] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 74212600 Paket 2: 74212728

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

Low

## Relative IP Identification number change

**Solution**
Contact your vendor for a patch

**Port**
general/tcp

---

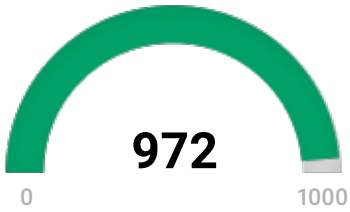
# 10.10.0.216

C8:1F:66:4B:97:51

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## DCE Services Enumeration

**Solution**

filter incoming traffic to this port.

**Port**

135/tcp

Medium

## DCE Services Enumeration

**Description**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this host: Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49664] Port: 49665/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: Impl friendly name UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: UserMgrCli UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: UserMgrCli UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: Adh APIs UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: IKE/Authip API UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: IdSegSrv service UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: AppInfo UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49665] Annotation: AppInfo Port: 49666/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49666] Annotation: Event log TCPIP UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49666] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49666] Annotation: NRP server endpoint Port: 49668/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49668] Named pipe : spoolss Win32 service or process : spoolsv.exe Description :

Spooler service UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49668] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49668] UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49668] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49668] Port: 49670/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.216[49670] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.10.0.216[49670] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49670] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.216[49670] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49670] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49670] Annotation: Ngc Pop Key Service Port: 49703/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49703] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.10.0.216[49703] Annotation: KeyIso UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49703] Annotation: Ngc Pop Key Service UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:10.10.0.216[49703] Annotation: Ngc Pop Key Service Port: 49705/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.10.0.216[49705] Solution : filter incoming traffic to this port(s).

**Solution**
filter incoming traffic to this port.

**Port**
135/tcp

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 258624610 Paket 2: 258625900

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

Low

## Relative IP Identification number change

**Solution**
Contact your vendor for a patch

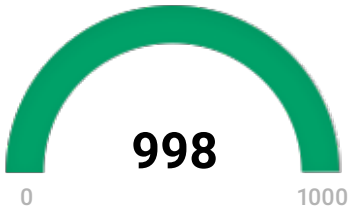
**Port**
general/tcp

---

# 10.10.0.218

C0:3F:D5:6E:33:5E

MAC Vendor **Elitegroup Computer Systems**
Hostname **N/A**
First Discovered **02/01/2017 22:49**




Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1120998217 Paket 2: 1120999567

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

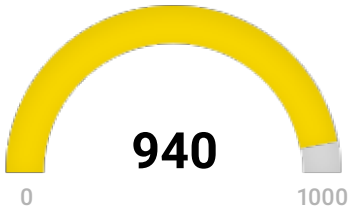
# 10.10.0.253

BC:30:5B:9B:23:65

MAC Vendor **Dell**

Hostname **N/A**

First Discovered **02/01/2017 22:49**




Medium

## Check for SSL Weak Ciphers

**Description**

Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA SSL3_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA TLS_1_2_RSA_WITH_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_MD5

**Solution**

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

**CVE**

CVE-2016-2183

**Port**

9390/tcp

---

Medium

## POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

**Solution**

Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0

**CVE**

CVE-2014-3566

**Port**

9390/tcp

**More Information**

https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

Medium

## Deprecated SSLv2 and SSLv3 Protocol Detection

**Description**

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

**Solution**

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Port**
9390/tcp

**More Information**
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/

---

Medium

## SSH Weak Encryption Algorithms Supported

**Description**
The following weak client-to-server encryption algorithms are supported by the remote service: aes192-cbc aes256-cbc arcfour128 arcfour aes128-cbc 3des-cbc arcfour256 rijndael-cbc@lysator.liu.se cast128-cbc blowfish-cbc The following weak server-to-client encryption algorithms are supported by the remote service: aes192-cbc aes256-cbc arcfour128 arcfour aes128-cbc 3des-cbc arcfour256 rijndael-cbc@lysator.liu.se cast128-cbc blowfish-cbc

**Solution**
Disable the weak encryption algorithms.

**Port**
22/tcp

**More Information**
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

---

Low

## TCP timestamps

**Description**
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1709265209 Paket 2: 1709265549

**Solution**
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

**Port**
general/tcp

**More Information**
http://www.ietf.org/rfc/rfc1323.txt

---

Low

## SSH Weak MAC Algorithms Supported

**Description**
The following weak client-to-server MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-sha1-96 hmac-md5-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-sha1-96-etm@openssh.com The following weak server-to-client MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-sha1-96 hmac-md5-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-sha1-96-etm@openssh.com

**Solution**
Disable the weak MAC algorithms

Disable the weak MAC algorithms.

**Port**
22/tcp

---