CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.
Table of Contents

1 - Summary
2 - Details
  2.1 - 10.0.1.1
  2.2 - 10.0.7.0
  2.3 - 10.0.7.1 (WIN-E4I89BKS3I8)
  2.4 - 10.0.7.2
  2.5 - 10.0.7.3
  2.6 - 10.0.7.4
  2.7 - 10.0.7.5
  2.8 - 10.0.7.6 (BO-SANDBOX)
  2.9 - 10.0.7.7
  2.10 - 10.0.7.8
  2.11 - 10.0.7.9
  2.12 - 10.0.7.10 (JIM-WIN7)
  2.13 - 10.0.7.11
  2.14 - 10.0.7.12 (CERTEXAM)
  2.15 - 10.0.7.13 (DEV-WIN8)
  2.16 - 10.0.7.14 (CONFERENCE_ROOM)
  2.17 - 10.0.7.15
  2.18 - 10.0.7.16 (DEVSYMATEC)
1 - Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.1</td>
<td>541</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9.0</td>
</tr>
<tr>
<td>10.0.7.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.1 (WIN-E4I89BKS3I8)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.6 (BO-SANDBOX)</td>
<td>13</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>9.3</td>
</tr>
<tr>
<td>10.0.7.7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.9</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>10.0.7.10 (JIM-WIN7)</td>
<td>14</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>10.0.7.11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>10.0.7.12 (CERTEXAM)</td>
<td>19</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>10.0.7.13 (DEV-WIN8)</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>10.0.7.14 (CONFERENCE_ROOM)</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>10.0.7.15</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>10.0.7.16 (DEVSYMANTEC)</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>10.0.7.17 (BOSIER-DT)</td>
<td>14</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>10.0</td>
</tr>
<tr>
<td>10.0.7.18 (PSOLER-WIN764)</td>
<td>30</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>10.0</td>
</tr>
<tr>
<td>10.0.7.19 (INSIP-DEV1)</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>10.0.7.20 (EHARRIS-WIN7)</td>
<td>16</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>10.0.7.255</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Total: 257</td>
<td>1977</td>
<td>88</td>
<td>192</td>
<td>50</td>
<td>0</td>
<td>10.0</td>
</tr>
</tbody>
</table>
# Issues by NVT (continued)

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHP Sessions Subsystem Session Fixation Vulnerability</td>
<td>2</td>
</tr>
<tr>
<td>PHP XML Handling Heap Buffer Overflow Vulnerability</td>
<td>2</td>
</tr>
<tr>
<td>PHP Remote Code Execution and Denial of Service Vulnerability</td>
<td>2</td>
</tr>
<tr>
<td>PHP phar.tar.c Heap Buffer Overflow Vulnerability</td>
<td>2</td>
</tr>
<tr>
<td>PHP Multiple Vulnerabilities -March 2013 (Windows)</td>
<td>2</td>
</tr>
<tr>
<td>PHP _php_stream_scandir() Buffer Overflow Vulnerability</td>
<td>2</td>
</tr>
<tr>
<td>Use LDAP search request to retrieve information from servers</td>
<td>1</td>
</tr>
<tr>
<td>LDAP allows null bases</td>
<td>1</td>
</tr>
<tr>
<td>Squid Header-Only Packets Remote Denial of Service</td>
<td>1</td>
</tr>
<tr>
<td>Squid HTCP Packets Processing Denial of Service</td>
<td>1</td>
</tr>
<tr>
<td>Squid External Auth Header Parser DOS Vulnerability</td>
<td>1</td>
</tr>
<tr>
<td>Squid information-disclosure vulnerability</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft IIS Default Welcome Page Information Disclosure</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft IIS IP Address/Internal Network Name Disclosure</td>
<td>1</td>
</tr>
<tr>
<td>Windows Administrator NULL FTP password</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft IIS FTPd NLST stack overflow</td>
<td>1</td>
</tr>
<tr>
<td>Check for SSL Weak Ciphers</td>
<td>1</td>
</tr>
<tr>
<td>Citrix published applications</td>
<td>1</td>
</tr>
<tr>
<td>MySQL ALTER DATABASE Remote Denial Of Service Vulnerability</td>
<td>1</td>
</tr>
<tr>
<td>MySQL Empty Bit-String Literal Denial of Service Vulnerability</td>
<td>1</td>
</tr>
<tr>
<td>Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service</td>
<td>1</td>
</tr>
<tr>
<td>Oracle MySQL TEMPORARY InnoDB Tables Denial Of Service</td>
<td>1</td>
</tr>
<tr>
<td>MySQL MyISAM Table Privileges Security Bypass Vulnerability</td>
<td>1</td>
</tr>
<tr>
<td>MySQL Authenticated Access Restrictions Bypass Vulnerability</td>
<td>1</td>
</tr>
<tr>
<td>MySQL multiple Vulnerabilities</td>
<td>1</td>
</tr>
</tbody>
</table>
2 - Scan Details

Issues by Severity

- High: 88
- Medium: 192
- Low: 50
- False Positive: 0
Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.6 (BO-SANDBOX)</td>
<td>13</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>9.3</td>
</tr>
</tbody>
</table>

Listening Ports

Port

135/tcp (loc-srv), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 3389/tcp, 5357/tcp, 47001/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49176/tcp, 49194/tcp, 59650/tcp, 137/udp (netbios-ns)

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)</td>
<td>3389/tcp</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9.3</td>
</tr>
<tr>
<td>Microsoft RDP Server Private Key Information Disclosure Vulnerability</td>
<td>3389/tcp</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>DCE Services Enumeration</td>
<td>135/tcp (loc-srv)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>TCP timestamps</td>
<td>135/tcp</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

**High (CVSS: 9.3)**

<table>
<thead>
<tr>
<th>Port</th>
<th>3389/tcp</th>
</tr>
</thead>
</table>

**NVT:** Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387) (OID: 1.3.6.1.4.1.25623.1.0.902818)

**Summary**

This host is missing a critical security update according to Microsoft Bulletin MS12-020.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user or cause a denial of service condition. Impact Level: System/Application
**Solution**
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms12-020

**Vulnerability Insight**
The flaws are due to the way Remote Desktop Protocol accesses an object in memory that has been improperly initialized or has been deleted and the way RDP service processes the packets.

**Vulnerability Detection Method**
Details: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (267... (OID: 1.3.6.1.4.1.25623.1.0.902818)
Version used: $Revision: 174 $

**References**

**Medium (CVSS: 6.4)**
**3389/tcp**

**Summary**
This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation could allow remote attackers to gain sensitive information. Impact Level: System/Application

**Solution**
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A Workaround is to connect only to terminal services over trusted networks.

**Vulnerability Insight**
The flaw is due to RDP server which stores an RSA private key used for signing a terminal server’s public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

**Vulnerability Detection Method**
Details: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) Version used: $Revision: 283 $

**References**

**Medium (CVSS: 5)**
**135/tcp (loc-srv)**

**Summary**
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.

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.
Vulnerability Detection Result

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Summary

NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Low (CVSS: 2.6)

NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

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.

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.
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 718471216 Paket 2: 718471326

<table>
<thead>
<tr>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>A side effect of this feature is that the uptime of the remote host can sometimes be computed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>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: <a href="http://www.microsoft.com/en-us/download/details.aspx?id=9152">http://www.microsoft.com/en-us/download/details.aspx?id=9152</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>The remote host implements TCP timestamps, as defined by RFC1323.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability Detection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96 $</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
</table>
2.9 - 10.0.7.7

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected
2.10 - 10.0.7.8

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected
2.11 - 10.0.7.9

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.9</td>
<td></td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Listening Ports

Port

33003/tcp, 67/udp (bootps), 68/udp (bootpc), 1900/udp

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP timestamps</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

**Low (CVSS: 2.6)**

**NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)**

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Vulnerability Detection Result**

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 second in-between: Paket 1: 19641681 Paket 2: 19641793

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**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
### Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

### Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96$

### References
http://www.ietf.org/rfc/rfc1323.txt
2.12 - 10.0.7.10 (JIM-WIN7)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.10 (JIM-WIN7)</td>
<td>14</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>5.0</td>
</tr>
</tbody>
</table>

Listening Ports

<table>
<thead>
<tr>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>135/tcp (loc-srv), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 3389/tcp, 5357/tcp, 18086/tcp, 29100/tcp, 47001/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49183/tcp, 49185/tcp, 137/udp (netbios-ns)</td>
</tr>
</tbody>
</table>

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCE Services Enumeration</td>
<td>135/tcp (loc-srv)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>TCP timestamps</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

**Medium (CVSS: 5)**

NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

**Summary**

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.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Solution**

Filter incoming traffic to this port.

**Vulnerability Detection Method**

Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $
Summary
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.

Vulnerability Detection Result
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 |
| Port: 49153/tcp | UUID: f6beaff7-1e19-4fbf-9f9f-b89e2018337c, version 1 |

Solution
Filter incoming traffic to this port.

Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41$

Low (CVSS: 2.6)
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in between:

Paket 1: 99192916
Paket 2: 99193030

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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 timestamp=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

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.
### Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96$

### References
http://www.ietf.org/rfc/rfc1323.txt
2.13 - 10.0.7.11

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.11</td>
<td>0 0 0 0 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Listening Ports

*None detected*

NVT Issues Summary

*None detected*

Security Issues

*None detected*
2.15 - 10.0.7.13 (DEV-WIN8)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.13 (DEV-WIN8)</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
</tbody>
</table>

Listening Ports

<table>
<thead>
<tr>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>3389/tcp, 5357/tcp, 137/udp (netbios-ns)</td>
</tr>
</tbody>
</table>

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft RDP Server Private Key Information Disclosure</td>
<td>3389/tcp</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>TCP timestamps</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

<table>
<thead>
<tr>
<th>Medium (CVSS: 6.4)</th>
<th>3389/tcp</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)</td>
<td></td>
</tr>
</tbody>
</table>

Summary

This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote attackers to gain sensitive information. Impact Level: System/Application

Solution

No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A Workaround is to connect only to terminal services over trusted networks.

Vulnerability Insight
The flaw is due to RDP server which stores an RSA private key used for signing a terminal server’s public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

## Vulnerability Detection Method

**Details:** Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) Version used: $Revision: 283$

### References


<table>
<thead>
<tr>
<th>Low (CVSS: 2.6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)</td>
</tr>
</tbody>
</table>

### Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

### Vulnerability Detection Result

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 648705753 Paket 2: 648705866

### Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### 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](http://www.microsoft.com/en-us/download/details.aspx?id=9152)

### Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

---

<table>
<thead>
<tr>
<th><strong>Vulnerability Detection Method</strong></th>
</tr>
</thead>
</table>
| Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96$

### References

http://www.ietf.org/rfc/rfc1323.txt
2.16 - 10.0.7.14 (CONFERENCE_ROOM)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.14 (CONFERENCE_ROOM)</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
</tbody>
</table>

Listening Ports

Port

135/tcp (loc-srv), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 3389/tcp, 47001/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49173/tcp, 49176/tcp, 137/udp (netbios-ns)

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft RDP Server Private Key Information Disclosure</td>
<td>3389/tcp</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>DCE Services Enumeration</td>
<td>135/tcp (loc-srv)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>TCP timestamps</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

Medium (CVSS: 6.4) 3389/tcp

NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.9028658)

Summary
This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to gain sensitive information. Impact Level: System/Application

Solution
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A Workaround is to connect only to terminal services over trusted networks.
Vulnerability Insight
The flaw is due to RDP server which stores an RSA private key used for signing a terminal server's public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

Vulnerability Detection Method
Details: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) Version used: $Revision: 283$

References

Medium (CVSS: 5)
NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

Summary
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.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41$

Medium (CVSS: 5)
NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

Summary
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.

Vulnerability Detection Result
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.

Solution
filter incoming traffic to this port.
Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $

Low (CVSS: 2.6)
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 81676086 Paket 2: 81676200

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96 $

References
http://www.ietf.org/rfc/rfc1323.txt
2.17 - 10.0.7.15

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.15</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Listening Ports

Port
88/tcp (kerberos), 443/tcp (https), 888/tcp, 48230/tcp, 50021/tcp, 65534/tcp, 3702/udp, 10000/udp (webmin)

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP timestamps</td>
<td>50021/tcp</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>FTP Server type and version</td>
<td>50021/tcp</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1.9</td>
</tr>
</tbody>
</table>

Security Issues

**Low (CVSS: 2.6)**
NVT: TCP timestamps
(OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 899750831 Paket 2: 899750942

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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 cannot 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
### Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

### Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96 $

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

<table>
<thead>
<tr>
<th>Low (CVSS: 1.9)</th>
<th>50021/tcp</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVT: FTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10092)</td>
<td></td>
</tr>
</tbody>
</table>

### Summary
This detects the FTP Server type and version by connecting to the server and processing the buffer received. The login banner gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

### Vulnerability Detection Result
Remote FTP server banner: 220---------- Welcome to Pure-FTPD [privsep] ----------

### Solution
Change the login banner to something generic.

### Vulnerability Detection Method
Details: FTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10092) Version used: $Revision: 41 $
2.22 - 10.0.7.20 (EHARRIS-WIN7)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Hightest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.20 (EHARRIS-WIN7)</td>
<td>16</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>6.4</td>
</tr>
</tbody>
</table>

Listening Ports

Port

- 135/tcp (loc-srv), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 3389/tcp, 5357/tcp, 18086/tcp, 20121/tcp, 29080/tcp, 29081/tcp, 47001/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49229/tcp, 137/udp (netbios-ns)

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft RDP Server Private Key Information Disclosure Vulnerability</td>
<td>3389/tcp</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>DCE Services Enumeration</td>
<td>135/tcp (loc-srv)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>TCP timestamps</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

**Medium (CVSS: 6.4)**

**NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)**

**Summary**
This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation could allow remote attackers to gain sensitive information. Impact Level: System/Application

**Solution**
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A Workaround is to connect only to terminal services over trusted networks.
Vulnerability Insight
The flaw is due to RDP server which stores an RSA private key used for signing a terminal server's public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

Vulnerability Detection Method
Details: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) Version used: $Revision: 283 $

References

Medium (CVSS: 5)

<table>
<thead>
<tr>
<th>NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)</th>
<th>135/tcp (loc-srv)</th>
</tr>
</thead>
</table>

Summary
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.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $

Medium (CVSS: 5)

<table>
<thead>
<tr>
<th>NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)</th>
<th>135/tcp (loc-srv)</th>
</tr>
</thead>
</table>

Summary
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.

Vulnerability Detection Result
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.

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $

Medium (CVSS: 5)

<table>
<thead>
<tr>
<th>NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)</th>
<th>135/tcp (loc-srv)</th>
</tr>
</thead>
</table>

Summary
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.

Vulnerability Detection Result
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.

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $
<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solution</strong></td>
<td>filter incoming traffic to this port.</td>
</tr>
<tr>
<td><strong>Vulnerability Detection Method</strong></td>
<td>Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $</td>
</tr>
<tr>
<td><strong>Low (CVSS: 2.6)</strong></td>
<td>NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>The remote host implements TCP timestamps and therefore allows to compute the uptime.</td>
</tr>
<tr>
<td><strong>Vulnerability Detection Result</strong></td>
<td>It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 267384 Paket 2: 267496</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>A side effect of this feature is that the uptime of the remote host can sometimes be computed.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>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: <a href="http://www.microsoft.com/en-us/download/details.aspx?id=9152">http://www.microsoft.com/en-us/download/details.aspx?id=9152</a></td>
</tr>
<tr>
<td><strong>Vulnerability Insight</strong></td>
<td>The remote host implements TCP timestamps, as defined by RFC1323.</td>
</tr>
<tr>
<td><strong>Vulnerability Detection Method</strong></td>
<td>Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96 $</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td><a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a></td>
</tr>
</tbody>
</table>
2.30 - 10.0.7.28 (TERMINUS)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Hightest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.7.28 (TERMINUS)</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>10.0</td>
</tr>
</tbody>
</table>

Listening Ports

Port

- 135/tcp (loc-srv)
- 139/tcp (netbios-ssn)
- 445/tcp (microsoft-ds)
- 2002/tcp
- 3389/tcp
- 5357/tcp
- 29080/tcp
- 29100/tcp
- 47001/tcp
- 49192/tcp
- 49153/tcp
- 49154/tcp
- 49192/tcp
- 49197/tcp
- 137/udp (netbios-ns)

NVT Issues Summary

<table>
<thead>
<tr>
<th>NVT</th>
<th>Port</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Highest CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan horses</td>
<td>2002/tcp</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10.0</td>
</tr>
<tr>
<td>Microsoft RDP Server Private Key Information Disclosure Vulnerability</td>
<td>3389/tcp</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6.4</td>
</tr>
<tr>
<td>DCE Services Enumeration</td>
<td>135/tcp (loc-srv)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5.0</td>
</tr>
<tr>
<td>TCP timestamps</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Security Issues

High (CVSS: 10)

NVT: Trojan horses (OID: 1.3.6.1.4.1.25623.1.0.11157)

Summary

An unknown service runs on this port. It is sometimes opened by Trojan horses. Unless you know for sure what is behind it, you’d better check your system.

Vulnerability Detection Result

An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): \tSingu \tSlapper \tW32.Beagle

Unless you know for sure what is behind it, you’d better check your system.

Anyway, don’t panic, OpenVAS only found an open port. It may *** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner

Solution
if a trojan horse is running, run a good antivirus scanner

**Vulnerability Detection Method**

Details: Trojan horses (OID: 1.3.6.1.4.1.25623.1.0.11157) Version used: $Revision: 17$

### Medium (CVSS: 6.4)

**3389/tcp**

**NVT:** Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)

**Summary**

This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

Successful exploitation could allow remote attackers to gain sensitive information. Impact Level: System/Application

**Solution**

No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A Workaround is to connect only to terminal services over trusted networks.

**Vulnerability Insight**

The flaw is due to RDP server which stores an RSA private key used for signing a terminal server’s public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

**Vulnerability Detection Method**

Details: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) Version used: $Revision: 283$

**References**


### Medium (CVSS: 5)

**135/tcp (loc-srv)**

**NVT:** DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

**Summary**

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.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Solution**

filter incoming traffic to this port.

**Vulnerability Detection Method**

Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41$

**References**

Vulnerability Detection Result

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.

Solution

filter incoming traffic to this port.

Vulnerability Detection Method

Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 41 $

Low (CVSS: 2.6)

NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 36477545 Paket 2: 36477655

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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
**Vulnerability Insight**  
The remote host implements TCP timestamps, as defined by RFC1323.

**Vulnerability Detection Method**  
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 96$

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