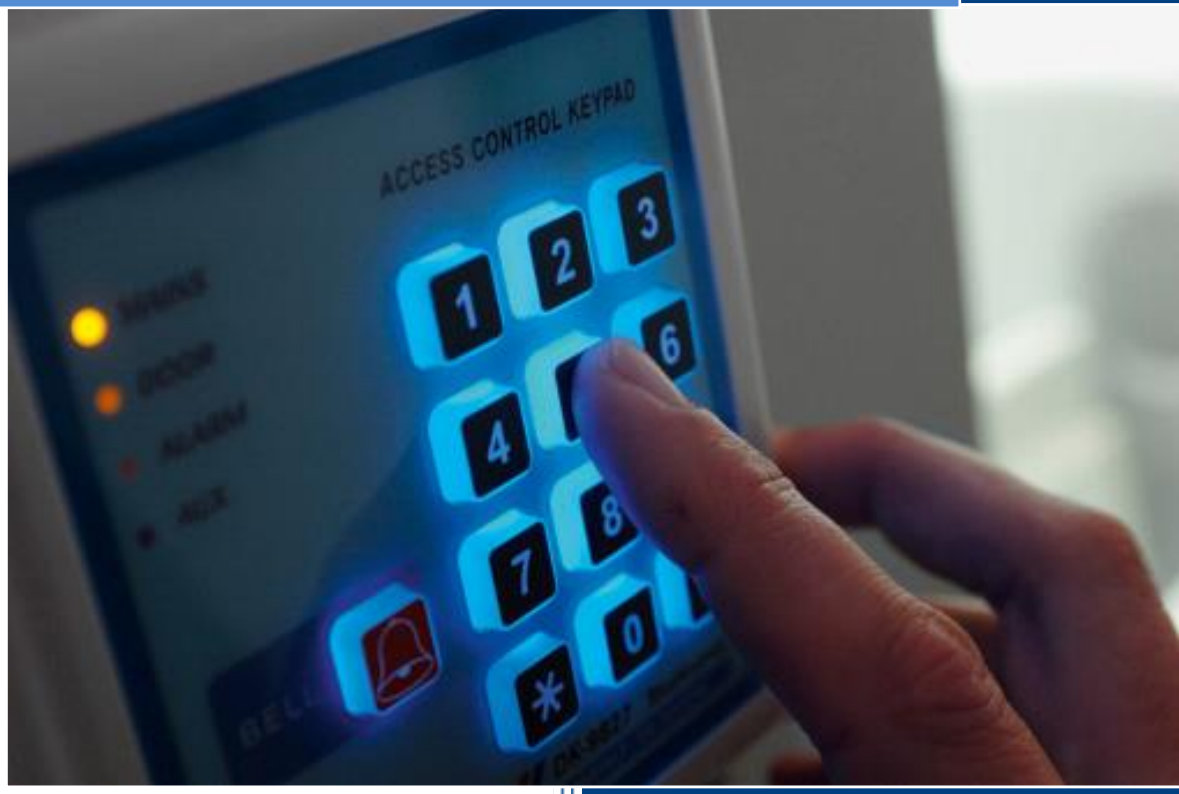
YourIT!
Your Logo Goes Here

Inspector Assessment

Internal Vulnerability Scan Detail Report

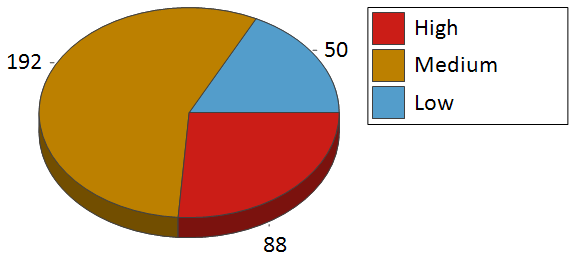


Prepared for:
Prospect Or Customer
Prepared by:
Your Company Name

Table of Contents

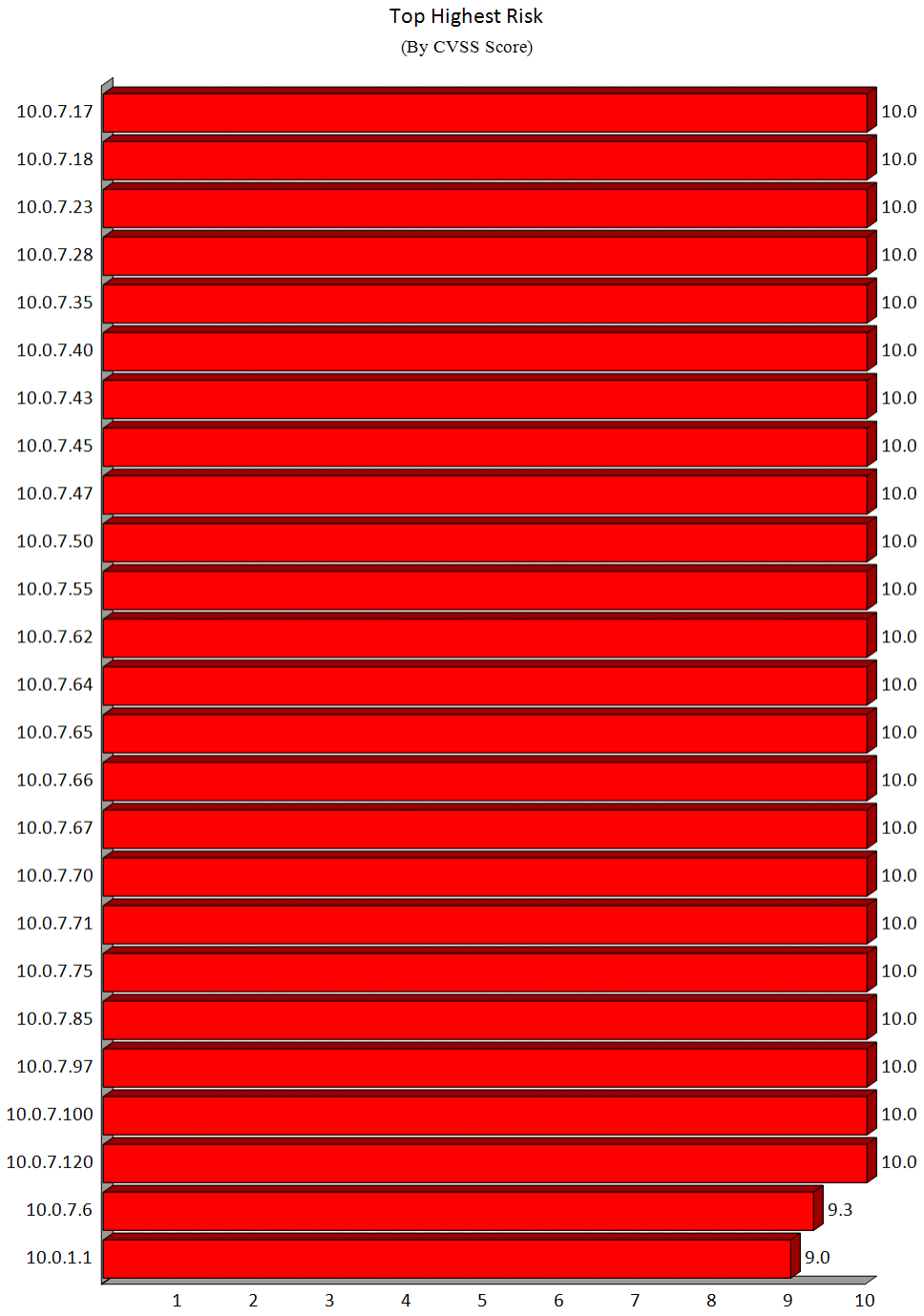
1 - Summary

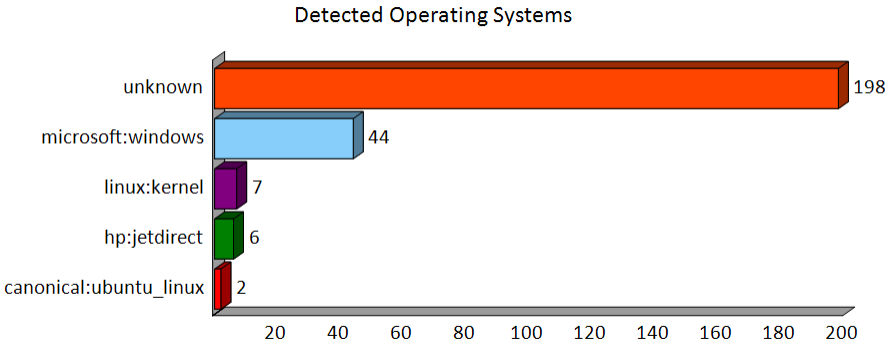
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.

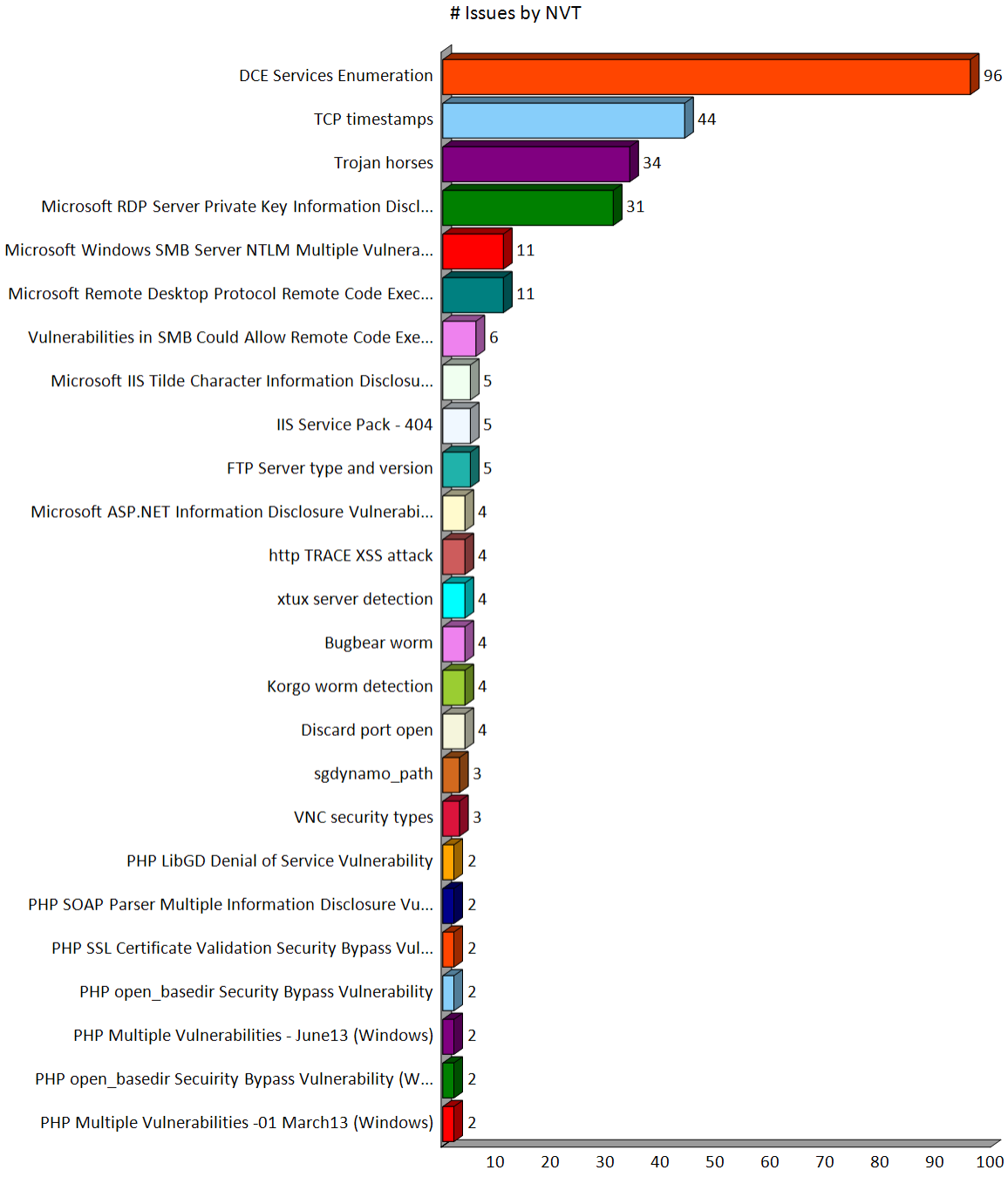


Host Issue Summary

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

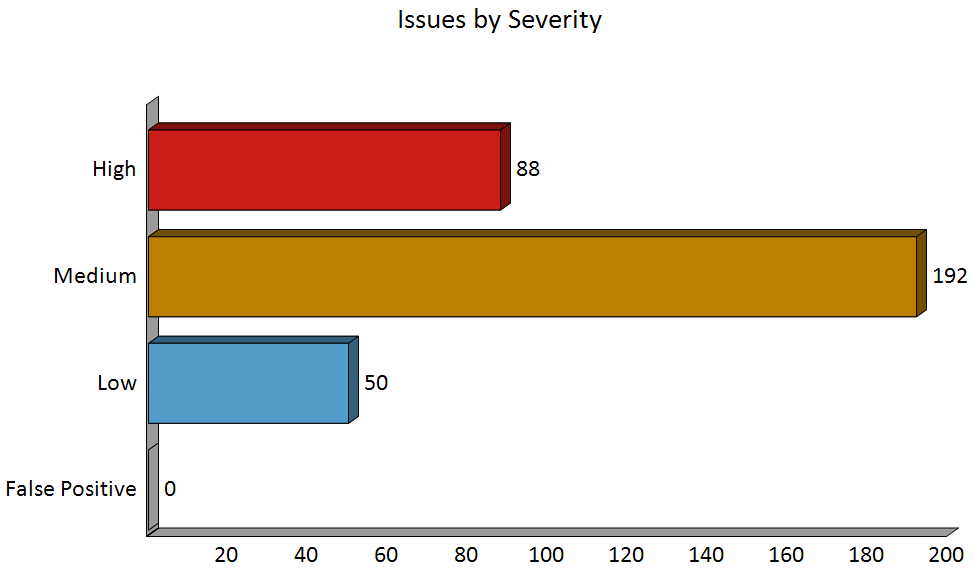

Top Highest Risk
(By CVSS Score)
10.0.7.17
10.0.7.18
10.0.7.23
10.0.7.28
10.0.7.35
10.0.7.40
10.0.7.43
10.0.7.45
10.0.7.47
10.0.7.50
10.0.7.55
10.0.7.62
10.0.7.64
10.0.7.65
10.0.7.66
10.0.7.67
10.0.7.70
10.0.7.71
10.0.7.75
10.0.7.85
10.0.7.97
10.0.7.100
10.0.7.120
10.0.7.6
10.0.1.1
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
10.0
9.3
9.0
1
2
3
4
5
6
7
8
9
10


Detected Operating Systems
unknown
198
microsoft:windows
44
linux:kernel
7
hp:jetdirect
6
canonical:ubuntu_linux
2
20
40
60
80
100
120
140
160
180
200

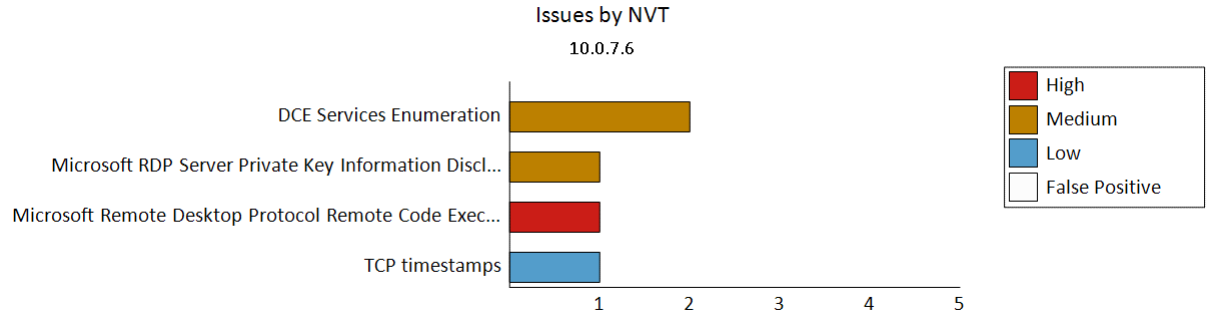

Issues by NVT
DCE Services Enumeration 96
TCP timestamps 44
Trojan horses 34
Microsoft RDP Server Private Key Information Discl... 31
Microsoft Windows SMB Server NTLM Multiple Vulnera... 11
Microsoft Remote Desktop Protocol Remote Code Exec... 11
Vulnerabilities in SMB Could Allow Remote Code Exe... 6
Microsoft IIS Tilde Character Information Disclosu... 5
IIS Service Pack - 404 5
FTP Server type and version 5
Microsoft ASP.NET Information Disclosure Vulnerabi... 4
http TRACE XSS attack 4
xtux server detection 4
Bugbear worm 4
Korgo worm detection 4
Discard port open 4
sgdynamo_path 3
VNC security types 3
PHP LibGD Denial of Service Vulnerability 2
PHP SOAP Parser Multiple Information Disclosure Vu... 2
PHP SSL Certificate Validation Security Bypass Vul... 2
PHP open_basedir Security Bypass Vulnerability 2
PHP Multiple Vulnerabilities - June13 (Windows) 2
PHP open_basedir Secuirity Bypass Vulnerability (W... 2
PHP Multiple Vulnerabilities -01 March13 (Windows) 2
10 20 30 40 50 60 70 80 90 100

Issues by NVT (continued)

2 - Scan Details



2.8 - 10.0.7.6 (BO-SANDBOX)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.6 (BO-SANDBOX)	13	1	3	1	0	9.3

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

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

Security Issues

High (CVSS: 9.3) 3389/tcp
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

http://blog.binaryninjas.org/?p=58, http://secunia.com/advisories/48395, http://support.microsoft.com/kb/2671387, http://www.securitytracker.com/id/1026790, http://technet.microsoft.com/en-us/security/bulletin/ms12-020

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

http://secunia.com/advisories/15605/, http://xforce.iss.net/xforce/xfdb/21954, http://www.oxid.it/downloads/rdp-gbu.pdf

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 $

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

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:10.0.7.6[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49153] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49153] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49153] Annotation: NRP server endpoint Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: XactSrv service UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: AppInfo UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] UUID: 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49154] Annotation: IKE/Authip API Port: 49176/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.0.7.6[49176] Port: 49194/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[49194] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 59650/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.0.7.6[59650] 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.

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: 718471216 Paket 2: 718471326

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

2.9 - 10.0.7.7

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.7	0	0	0	0	0	0.0

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected

2.10 - 10.0.7.8

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.8	0	0	0	0	0	0.0

Listening Ports

None detected

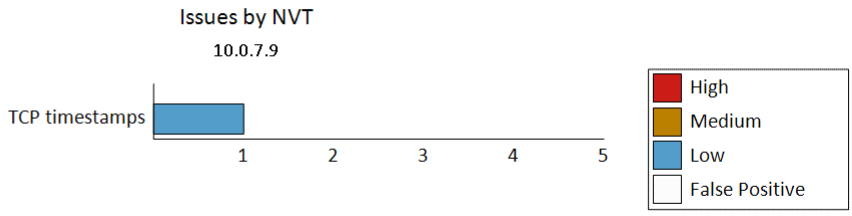
NVT Issues Summary

None detected

Security Issues

None detected

2.11 - 10.0.7.9



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.9	4	0	0	1	0	2.6

Listening Ports

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

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
TCP timestamps		0	0	1	0	2.6

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: 19641681 Paket 2: 19641793

Impact

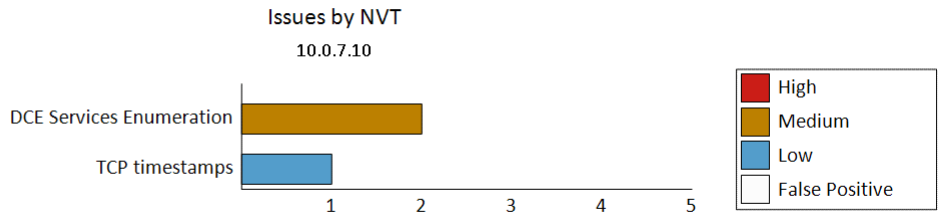
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.10 (JIM-WIN7)	14	0	2	1	0	5.0

Listening Ports

Port
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)

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
DCE Services Enumeration	135/tcp (loc-srv)	0	2	0	0	5.0
TCP timestamps		0	0	1	0	2.6

Security Issues

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 $

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

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:10.0.7.10[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49153] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49153] Annotation: Security Center Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49154] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49154] Annotation: XactSrv service UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49154] Port: 49183/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.7.10[49183] 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:10.0.7.10[49185] Solution : filter incoming traffic to this port(s).

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 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

2.13 - 10.0.7.11

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.11	0	0	0	0	0	0.0

Listening Ports

None detected

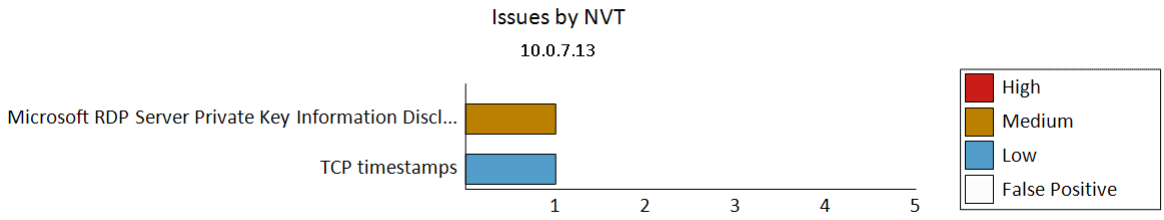
NVT Issues Summary

None detected

Security Issues

None detected

2.15 - 10.0.7.13 (DEV-WIN8)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.13 (DEV-WIN8)	3	0	1	1	0	6.4

Listening Ports

Port
3389/tcp, 5357/tcp, 137/udp (netbios-ns)

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
Microsoft RDP Server Private Key Information Disclosure Vulnerability	3389/tcp	0	1	0	0	6.4
TCP timestamps		0	0	1	0	2.6

Security Issues

Medium (CVSS: 6.4) 3389/tcp
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)

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

http://secunia.com/advisories/15605/, http://xforce.iss.net/xforce/xfdb/21954, http://www.oxid.it/downloads/rdp-gbu.pdf

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: 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

Vulnerability Insight

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

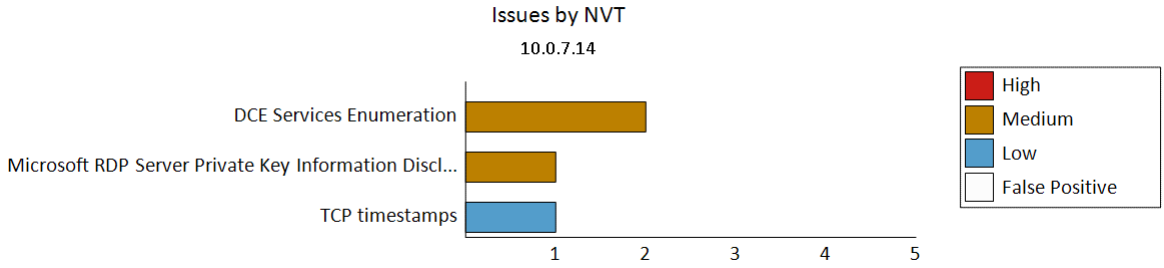
Vulnerability Detection Method

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

2.16 - 10.0.7.14 (CONFERENCE_ROOM)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.14 (CONFERENCE_ROOM)	12	0	3	1	0	6.4

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

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

Security Issues

Medium (CVSS: 6.4) 3389/tcp
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)

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

http://secunia.com/advisories/15605/, http://xforce.iss.net/xforce/xfdb/21954, http://www.oxid.it/downloads/rdp-gbu.pdf

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 $

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

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:10.0.7.14[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49153] Annotation: NRP server endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49153] Annotation: Wcm Service UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49153] Annotation: DHCP Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49153] Annotation: Security Center Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: IP Transition Configuration endpoint UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: Proxy Manager provider server endpoint UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: Adh APIs UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1

Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: XactSrv service UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: IdSegSrv service UUID: e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: Network Connection Broker server endpoint UUID: 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: KAPI Service endpoint UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Annotation: Impl friendly name UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] UUID: 9b008953-f195-4bf9-bde0-4471971e58ed, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49154] Port: 49155/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.0.7.14[49155] Annotation: RemoteAccessCheck UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.0.7.14[49155] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49173/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.7.14[49173] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49176/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.0.7.14[49176] Solution : filter incoming traffic to this port(s).

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.

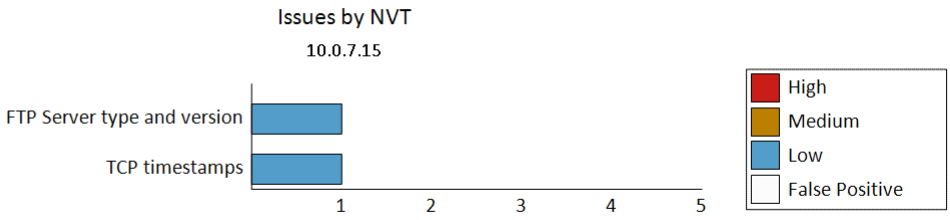
Vulnerability Detection Method

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

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.15	8	0	0	2	0	2.6

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

NVT	Port	High	Med	Low	False	Highest CVSS
TCP timestamps		0	0	1	0	2.6
FTP Server type and version	50021/tcp	0	0	1	0	1.9

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 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

Low (CVSS: 1.9) 50021/tcp
NVT: FTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10092)

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] ----------

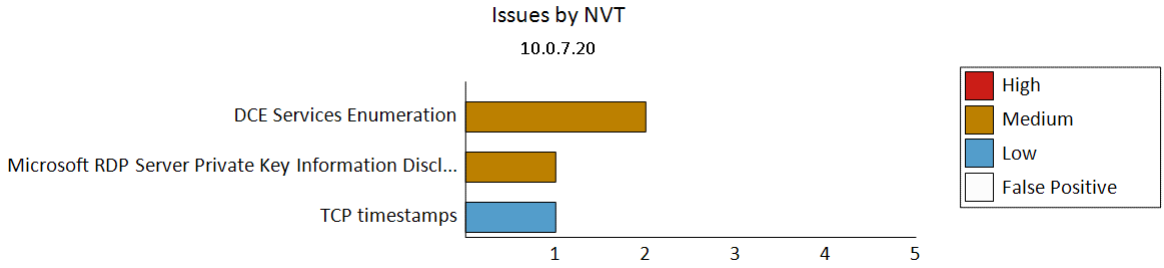
Solution

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

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.20 (EHARRIS-WIN7)	16	0	3	1	0	6.4

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

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

Security Issues

Medium (CVSS: 6.4) 3389/tcp
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)

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

http://secunia.com/advisories/15605/, http://xforce.iss.net/xforce/xfdb/21954, http://www.oxid.it/downloads/rdp-gbu.pdf

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 $

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

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:10.0.7.20[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49153] Annotation: Security Center Port: 49154/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49154] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49154] Annotation: KeyIso Port: 49155/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49155] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49155] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49155] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49155] Annotation: XactSrv service UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49155] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.7.20[49155] Annotation: Impl friendly name Port: 49229/tcp UUID: 367abb81-9844-35f1-ad32-

98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.0.7.20[49229] Solution : filter incoming traffic to this port(s).

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: 267384 Paket 2: 267496

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.

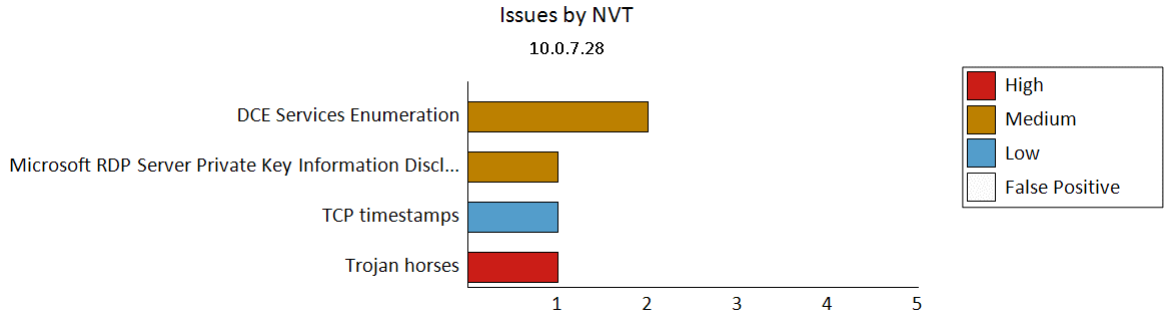
Vulnerability Detection Method

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

2.30 - 10.0.7.28 (TERMINUS)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
10.0.7.28 (TERMINUS)	15	1	3	1	0	10.0

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, 49152/tcp, 49153/tcp, 49154/tcp, 49192/tcp, 49197/tcp, 137/udp (netbios-ns)

NVT Issues Summary

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

Security Issues

High (CVSS: 10) 2002/tcp
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

http://secunia.com/advisories/15605/, http://xforce.iss.net/xforce/xfdb/21954, http://www.oxid.it/downloads/rdp-gbu.pdf

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 $

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

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:10.0.7.28[49152] Port: 49153/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49153] Annotation: Event log TCPIP UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49153] Annotation: Security Center Port: 49154/tcp UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: IKE/Authip API UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: IP Transition Configuration endpoint UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: XactSrv service UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: Impl friendly name UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: AppInfo UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: AppInfo UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Annotation: AppInfo UUID: 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49154] Port: 49192/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.7.28[49192] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49197/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.0.7.28[49197] Solution : filter incoming traffic to this port(s).

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