Scan Report

April 7, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "TargetsVPN Scan". The scan started at Wed Apr 3 00:27:07 2024 UTC and ended at Wed Apr 3 06:51:53 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.250.13 WIN2LAME	16	15	1	0	0
192.168.250.22	2	2	1	0	0
192.168.250.17	1	1	3	0	0
192.168.250.16	1	1	1	0	0
192.168.250.18	1	5	3	0	0
192.168.250.12	2	8	3	0	0
192.168.250.19	2	17	4	0	0
192.168.250.11	2	3	2	0	0
192.168.250.10	1	3	3	0	0
192.168.250.14	0	0	2	0	0
192.168.250.15	0	0	2	0	0
Total: 11	28	55	25	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 108 results selected by the filtering described above. Before filtering there were 813 results.

2 Results per Host

2.1 192.168.250.13

Host scan start	Wed Apr 3 00:28:32 2024 UTC
Host scan end	Wed Apr 3 02:40:07 2024 UTC

Service (Port)	Threat Level
80/tcp	High
9/tcp	High
119/tcp	High
3389/tcp	High
2103/tcp	High

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
42/tcp	High
445/tcp	High
21/tcp	High
161/udp	High
general/tcp	High
2397/tcp	High
80/tcp	Medium
17/tcp	Medium
19/tcp	Medium
7/udp	Medium
17/udp	Medium
137/udp	Medium
25/tcp	Medium
19/udp	Medium
7/tcp	Medium
21/tcp	Medium
general/icmp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)

NVT: Microsoft IIS .IDA ISAPI Filter Applied - Active Check

Product detection result
`cpe:/a:microsoft:internet_information_services:5.0`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:`
`↪ 1.3.6.1.4.1.25623.1.0.900710)`

Summary
Indexing Service filter is enabled on the remote Web server.

Quality of Detection: 70

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

Solution:
Solution type: Mitigation
To unmap the .IDA extension:
1.Open Internet Services Manager.
2.Right-click the Web server choose Properties from the context menu.
3.Master Properties

... continues on next page ...

... continued from previous page ...

4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .ida from the list.
In addition, you may wish to download and install URLSCAN from the Microsoft Technet web site. URLSCAN, by default, blocks all .ida requests to the IIS server.

Vulnerability Insight
The IIS server appears to have the .IDA ISAPI filter mapped.
At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033, and gives remote SYSTEM level access to the web server.
It is recommended that even if you have patched this vulnerability that you unmap the .IDA extension, and any other unused ISAPI extensions if they are not required for the operation of your site.

Vulnerability Detection Method
Details: `Microsoft IIS .IDA ISAPI Filter Applied - Active Check`
OID:1.3.6.1.4.1.25623.1.0.10695
Version used: `2023-10-10T05:05:41Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:5.0`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`cve: CVE-2001-0500`
`iava: 2001-a-0008`
`url: http://www.securityfocus.com/bid/2880`

High (CVSS: 10.0)

NVT: Microsoft Internet Information Services (IIS) End of Life (EOL) Detection

Product detection result
`cpe:/a:microsoft:internet_information_services:5.0`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:`
`↪ 1.3.6.1.4.1.25623.1.0.900710)`

Summary
The Microsoft Internet Information Services (IIS) version on the remote host has reached the end of life (EOL) and should not be used anymore.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
The "Internet Information Services (IIS)" version on the remote host has reached
↪ the end of life.
CPE:                cpe:/a:microsoft:internet_information_services:5.0
Installed version: 5.0
EOL version:        5.0
EOL date:           2010-07-13
```

Impact

An EOL version of Microsoft IIS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: VendorFix

The Microsoft IIS version is tightly coupled to the operation system on the remote host. Updating the operation system to a supported version is required.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.

Details: `Microsoft Internet Information Services (IIS) End of Life (EOL) Detection`

OID:1.3.6.1.4.1.25623.1.0.108114

Version used: `2024-02-28T14:37:42Z`

Product Detection Result

Product: `cpe:/a:microsoft:internet_information_services:5.0`

Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`

OID: 1.3.6.1.4.1.25623.1.0.900710)

References

```
url: https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Inte
↪rnet%20Information%20Services
```

High (CVSS: 7.5)

NVT: Microsoft IIS Directory Traversal Vulnerability (MS00-078) - Active Check

Product detection result

```
cpe:/a:microsoft:internet_information_services:5.0
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
↪ 1.3.6.1.4.1.25623.1.0.900710)
```

... continues on next page ...

... continued from previous page ...

Summary
The remote IIS server allows anyone to execute arbitrary commands by adding a unicode representation for the slash character in the requested path.

Quality of Detection: 70

Vulnerability Detection Result
`Vulnerable URL: http://192.168.250.13/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..`
`↪%c0%af../winnt/system32/cmd.exe?/c+dir+c:\+/OG`

Solution:
Solution type: VendorFix
The vendor has releases updates. Please see the references for more information.

Vulnerability Detection Method
Details: `Microsoft IIS Directory Traversal Vulnerability (MS00-078) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.10537
Version used: `2023-10-10T05:05:41Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:5.0`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`cve: CVE-2000-0884`
`iava: 2000-a-0005`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/ms`
`↪00-078`
`url: http://www.securityfocus.com/bid/1806`

[return to 192.168.250.13]

2.1.2 High 9/tcp

High (CVSS: 10.0)

NVT: Check for discard Service

Summary
The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.
This service is unused these days, so it is advised that you disable it.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
`The discard service was detected on the target host.`

Solution:
Solution type: Mitigation
- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0: HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard
Then launch cmd.exe and type:
net stop simptcp
net start simptcp
To restart the service.

Vulnerability Detection Method
Checks whether a discard service is exposed on the target host.
Details: `Check for discard Service`
OID:1.3.6.1.4.1.25623.1.0.11367
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0636`

[return to 192.168.250.13]

2.1.3 High 119/tcp

High (CVSS: 10.0)

NVT: Windows NT NNTP Component Buffer Overflow

Summary
The Network News Transfer Protocol (NNTP) component of Microsoft Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003, Exchange 2000 Server, and Exchange Server 2003 allows remote attackers to execute arbitrary code via XPAT patterns, possibly related to improper length validation and an unchecked buffer, leading to off-by-one and heap-based buffer overflows.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 5.0.2159.1
Fixed version: See referenced vendor advisory

Solution:
Solution type: VendorFix
Microsoft has released a bulletin that includes fixes to address this issue for supported versions of the operating system.

Vulnerability Detection Method
Details: Windows NT NNTP Component Buffer Overflow
OID:1.3.6.1.4.1.25623.1.0.100608
Version used: 2023-07-28T16:09:07Z

References
cve: CVE-2004-0574
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2004/ms04-036

[return to 192.168.250.13]

2.1.4 High 3389/tcp

High (CVSS: 9.3)

NVT: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387) - Active Check

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

Quality of Detection: 99

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.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
- Microsoft Windows 7 Service Pack 1 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 2K3 Service Pack 2 and prior
- Microsoft Windows Vista Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior

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 (267138.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902818
Version used: `2024-01-09T05:06:46Z`

References
`cve: CVE-2012-0002`
`cve: CVE-2012-0152`
`url: http://blog.binaryninjas.org/?p=58`
`url: http://www.securityfocus.com/bid/52353`
`url: http://www.securityfocus.com/bid/52354`
`url: http://support.microsoft.com/kb/2671387`
`url: http://www.securitytracker.com/id/1026790`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms`
`↪12-020`
`dfn-cert: DFN-CERT-2012-0477`

[return to 192.168.250.13]

2.1.5 High 2103/tcp

High (CVSS: 10.0)

NVT: Message Queuing Remote Code Execution Vulnerability (951071) - Remote

Summary
This host is missing important security update according to Microsoft Bulletin MS08-065.

Quality of Detection: 98

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

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation could allow remote code execution by sending a specially crafted RPC request and can take complete control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows 2000 Service Pack 4 and prior.

Vulnerability Insight
The flaw exists due to a boundary error when parsing RPC requests to the Message Queuing (MSMQ).

Vulnerability Detection Method
Details: `Message Queuing Remote Code Execution Vulnerability (951071) - Remote`
OID:1.3.6.1.4.1.25623.1.0.900244
Version used: `2022-05-02T09:35:37Z`

References
`cve: CVE-2008-3479`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms`
`↪08-065`
`url: http://www.securityfocus.com/bid/31637`

[return to 192.168.250.13]

2.1.6 High 42/tcp

High (CVSS: 9.3)

NVT: Microsoft Windows WINS Remote Code Execution Vulnerability (2524426)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS11-035.

Quality of Detection: 80

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

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation could allow remote attackers to execute arbitrary code with elevated privileges or cause a denial-of-service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2K3 Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
The flaw is caused by a logic error in the Windows Internet Name Service (WINS) when handling a socket send exception, which could cause certain user supplied values to remain within a stack frame and to be reused in another context, leading to arbitrary code execution with elevated privileges.

Vulnerability Detection Method
Details: `Microsoft Windows WINS Remote Code Execution Vulnerability (2524426)`
OID:1.3.6.1.4.1.25623.1.0.802260
Version used: `2023-07-28T05:05:23Z`

References
```
cve: CVE-2011-1248
url: http://xforce.iss.net/xforce/xfdb/67100
url: http://www.securityfocus.com/bid/47730
url: http://www.exploit-db.com/exploits/17830/
url: http://www.zerodayinitiative.com/advisories/ZDI-11-167/
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms
↪11-035
dfn-cert: DFN-CERT-2011-0737
```

[return to 192.168.250.13]

2.1.7 High 445/tcp

High (CVSS: 10.0)

NVT: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote

Summary
This host is missing a critical security update according to Microsoft Bulletin MS09-001.

Quality of Detection: 98

... continues on next page ...

... continued from previous page ...

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

Impact
Successful exploitation could allow remote unauthenticated attackers to cause denying the service by sending a specially crafted network message to a system running the server service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2K Service Pack 4 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 2003 Service Pack 2 and prior

Vulnerability Insight
The issue is due to the way Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Vulnerability Detection Method
Details: `Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote`
OID:1.3.6.1.4.1.25623.1.0.900233
Version used: `2022-05-02T09:35:37Z`

References
`cve: CVE-2008-4114`
`cve: CVE-2008-4834`
`cve: CVE-2008-4835`
`url: http://www.milw0rm.com/exploits/6463`
`url: http://www.securityfocus.com/bid/31179`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms`
`↪09-001`

High (CVSS: 10.0)

NVT: Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)

Summary
This host is missing important security update according to Microsoft Bulletin MS06-040.

Quality of Detection: 98

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote code execution by sending a specially crafted RPC request and can take complete control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP Service Pack 2 and prior
- Microsoft Windows 2K3 Service Pack 1 and prior
- Microsoft Windows 2000 Service Pack 4 and prior

Vulnerability Insight
The flaw is due to a boundary error in the 'CanonicalizePathName()' function in netapi32.dll and can be exploited to cause a stack-based buffer overflow via a malicious NetrpPathCanonicalize RPC request with an overly long path name to the Server Service.

Vulnerability Detection Method
Details: `Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)`
OID:1.3.6.1.4.1.25623.1.0.902782
Version used: `2022-04-28T13:38:57Z`

References
```
cve: CVE-2006-3439
url: http://securitytracker.com/id?1016667
url: http://www.securityfocus.com/bid/19409
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms
↪06-040
```

High (CVSS: 8.1)

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Quality of Detection: 95

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

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2017-0143`
`cve: CVE-2017-0144`
`cve: CVE-2017-0145`
`cve: CVE-2017-0146`
`cve: CVE-2017-0147`
`cve: CVE-2017-0148`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://support.microsoft.com/en-us/kb/4013078`
`url: http://www.securityfocus.com/bid/96703`
`url: http://www.securityfocus.com/bid/96704`
`url: http://www.securityfocus.com/bid/96705`
`url: http://www.securityfocus.com/bid/96707`
`url: http://www.securityfocus.com/bid/96709`
`url: http://www.securityfocus.com/bid/96706`
`url: https://technet.microsoft.com/library/security/MS17-010`

... continues on next page ...

... continued from previous page ...

url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448

[return to 192.168.250.13]

2.1.8 High 21/tcp

High (CVSS: 9.0)

NVT: Microsoft IIS FTPd NLST stack overflow

Summary
Microsoft IIS FTPd NLST stack overflow
The Microsoft IIS FTPd service may be vulnerable to a stack overflow via the NLST command. On Microsoft IIS 5.x this vulnerability can be used to gain remote SYSTEM level access, whilst on IIS 6.x it has been reported to result in a denial of service. Whilst it can be triggered by authenticated users with write access to the FTP server, this check determines whether anonymous users have the write access necessary to trigger it without authentication.

Quality of Detection: 80

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

Solution:
Solution type: Mitigation
We are not aware of a vendor approved solution at the current time.
On the following platforms, we recommend you mitigate in the described manner:
Microsoft IIS 5.x
Microsoft IIS 6.x
We recommend you mitigate in the following manner:
Filter inbound traffic to 21/tcp to only known management hosts Consider removing directories writable by 'anonymous'

Vulnerability Detection Method
Details: Microsoft IIS FTPd NLST stack overflow
OID:1.3.6.1.4.1.25623.1.0.100952
Version used: 2023-08-01T13:29:10Z

References
cve: CVE-2009-3023
url: http://www.securityfocus.com/bid/36189
dfn-cert: DFN-CERT-2009-1448

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2009-1228
```

[return to 192.168.250.13]

2.1.9 High 161/udp

High (CVSS: 7.6)

NVT: Report default community names of the SNMP Agent

Summary
Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE).

Quality of Detection: 99

Vulnerability Detection Result
`SNMP Agent responded as expected when using the following community name: public`

Impact
If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.
If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing network traffic, initiating processes, etc. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine.
Note that this test only gathers information and does not attempt to write to the remote device. Thus it is not possible to determine automatically whether the reported community is public or private.
Also note that information made available through a guessable community string might or might not contain sensitive data. Please review the information available through the reported community string to determine the impact of this disclosure.

Solution:
Solution type: VendorFix
Determine if the detected community string is a private community string. Determine whether a public community string exposes sensitive information. Disable the SNMP service if you don't use it or change the default community string.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details: Report default community names of the SNMP Agent
OID:1.3.6.1.4.1.25623.1.0.10264
Version used: 2023-11-02T05:05:26Z

References

cve: CVE-1999-0472
cve: CVE-1999-0516
cve: CVE-1999-0517
cve: CVE-1999-0792
cve: CVE-2000-0147
cve: CVE-2001-0380
cve: CVE-2001-0514
cve: CVE-2001-1210
cve: CVE-2002-0109
cve: CVE-2002-0478
cve: CVE-2002-1229
cve: CVE-2004-1474
cve: CVE-2004-1775
cve: CVE-2004-1776
cve: CVE-2011-0890
cve: CVE-2012-4964
cve: CVE-2014-4862
cve: CVE-2014-4863
cve: CVE-2016-1452
cve: CVE-2016-5645
cve: CVE-2017-7922
cve: CVE-2020-5364
url: http://www.securityfocus.com/bid/11237
url: http://www.securityfocus.com/bid/177
url: http://www.securityfocus.com/bid/20125
url: http://www.securityfocus.com/bid/2112
url: http://www.securityfocus.com/bid/2896
url: http://www.securityfocus.com/bid/3758
url: http://www.securityfocus.com/bid/3795
url: http://www.securityfocus.com/bid/3797
url: http://www.securityfocus.com/bid/41436
url: http://www.securityfocus.com/bid/4330
url: http://www.securityfocus.com/bid/46981
url: http://www.securityfocus.com/bid/5030
url: http://www.securityfocus.com/bid/5965
url: http://www.securityfocus.com/bid/7081
url: http://www.securityfocus.com/bid/7212
url: http://www.securityfocus.com/bid/7317
url: http://www.securityfocus.com/bid/91756
url: http://www.securityfocus.com/bid/92428
url: http://www.securityfocus.com/bid/9681
url: http://www.securityfocus.com/bid/973

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/986
url: http://www.securityfocus.com/bid/99083
cert-bund: CB-K18/1132
cert-bund: CB-K16/1061
dfn-cert: DFN-CERT-2016-1130
```

[return to 192.168.250.13]

2.1.10 High general/tcp

High (CVSS: 10.0)

NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result

```
cpe:/o:microsoft:windows_2000
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection: 80

Vulnerability Detection Result

```
The "Windows 2000" Operating System on the remote host has reached the end of li
↪fe.
CPE:                cpe:/o:microsoft:windows_2000
EOL date:           2010-07-13
EOL info:           https://support.microsoft.com/en-us/lifecycle/search/default.
↪aspx?sort=PN&alpha=Windows+2000&Filter=FilterNO
```

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: Mitigation

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if an EOL version of an OS is present on the target host.
Details: Operating System (OS) End of Life (EOL) Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: 2024-02-28T14:37:42Z

Product Detection Result
Product: cpe:/o:microsoft:windows_2000
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.250.13]

2.1.11 High 2397/tcp

High (CVSS: 10.0)

NVT: Microsoft Internet Information Services (IIS) End of Life (EOL) Detection

Product detection result
cpe:/a:microsoft:internet_information_services:5.0
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
↪ 1.3.6.1.4.1.25623.1.0.900710)

Summary
The Microsoft Internet Information Services (IIS) version on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection: 80

Vulnerability Detection Result
The "Internet Information Services (IIS)" version on the remote host has reached
↪ the end of life.
CPE: cpe:/a:microsoft:internet_information_services:5.0
Installed version: 5.0
EOL version: 5.0
EOL date: 2010-07-13

Impact
An EOL version of Microsoft IIS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

The Microsoft IIS version is tightly coupled to the operation system on the remote host. Updating the operation system to a supported version is required.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: `Microsoft Internet Information Services (IIS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.108114
Version used: `2024-02-28T14:37:42Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:5.0`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`url: https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Inte`
`↪rnet%20Information%20Services`

High (CVSS: 7.5)

NVT: Microsoft Internet Information Services (IIS) XSS via 404 error

Product detection result
`cpe:/a:microsoft:internet_information_services:5.0`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:`
`↪ 1.3.6.1.4.1.25623.1.0.900710)`

Summary
This IIS Server appears to vulnerable to one of the cross site scripting attacks described in MS02-018.

Quality of Detection: 70

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

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the 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.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The default '404' file returned by IIS uses scripting to output a link to top level domain part of the url requested. By crafting a particular URL it is possible to insert arbitrary script into the page for execution.
The presence of this vulnerability also indicates that the host is vulnerable to the other issues identified in MS02-018 (various remote buffer overflow and cross site scripting attacks...)

Vulnerability Detection Method
Details: `Microsoft Internet Information Services (IIS) XSS via 404 error`
OID:1.3.6.1.4.1.25623.1.0.10936
Version used: `2023-10-10T05:05:41Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:5.0`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`cve: CVE-2002-0148`
`cve: CVE-2002-0150`
`iava: 2002-A-0002`
`url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/ms`
`↪02-018`
`url: http://www.securityfocus.com/bid/4476`
`url: http://www.securityfocus.com/bid/4483`
`url: http://www.securityfocus.com/bid/4486`
`url: http://jscript.dk/adv/TL001/`

[return to 192.168.250.13]

2.1.12 Medium 80/tcp

Medium (CVSS: 5.8)

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Quality of Detection: 99

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE TRACK`

... continues on next page ...

... continued from previous page ...

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

References
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`
`url: http://www.securityfocus.com/bid/24456`
`url: http://www.securityfocus.com/bid/33374`
`url: http://www.securityfocus.com/bid/36956`
`url: http://www.securityfocus.com/bid/36990`
`url: http://www.securityfocus.com/bid/37995`
`url: http://www.securityfocus.com/bid/9506`
`url: http://www.securityfocus.com/bid/9561`

... continues on next page ...

... continued from previous page ...

```
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.0)

NVT: Microsoft Internet Information Services (IIS) Service Pack - 404

Product detection result

```
cpe:/a:microsoft:internet_information_services:5.0
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
↪ 1.3.6.1.4.1.25623.1.0.900710)
```

Summary

Ensure that the server is running the latest stable Service Pack

Quality of Detection: 80

Vulnerability Detection Result

```
The remote IIS server *seems* to be Microsoft IIS 5 - SP0 or SP1
```

Solution:

Solution type: VendorFix

The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk.

Caveat: This test makes assumptions of the remote patch level based on static return values (Content-Length) within the IIS Servers 404 error message. As such, the test can not be totally reliable and should be manually confirmed.

Vulnerability Detection Method

Details: `Microsoft Internet Information Services (IIS) Service Pack - 404`

OID:1.3.6.1.4.1.25623.1.0.11874

Version used: `2023-10-10T05:05:41Z`

Product Detection Result

Product: `cpe:/a:microsoft:internet_information_services:5.0`

Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`

... continues on next page ...

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.900710)

Medium (CVSS: 5.0)

NVT: Microsoft IIS 5.0 PROPFIND DoS Vulnerability (MS01-016) - Active Check

Product detection result
`cpe:/a:microsoft:internet_information_services:5.0`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:`
`↪ 1.3.6.1.4.1.25623.1.0.900710)`

Summary
Microsoft Internet Information Services (IIS) server is prone to a denial of service (DoS) vulnerability.

Quality of Detection: 70

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

Impact
An attacker, exploiting this vulnerability, would be able to render the web service useless. If the server is 'business critical', the impact could be high.

Solution:
Solution type: Mitigation
Disable the WebDAV extensions, as well as the PROPFIND command.
Please see the references for more information.

Affected Software/OS
Microsoft IIS 5.0 is known to be affected.

Vulnerability Insight
It was possible to disable the remote IIS server by making a variation of a specially formed PROPFIND request.

Vulnerability Detection Method
Depending on the 'safe_checks' setting of the scan configuration:
- Setting 'yes': Sends a crafted HTTP PROPFIND request and checks if the response is matching one of an affected system
- Setting 'no': Sends a crafted HTTP PROPFIND request and checks if the system is still responding afterwards
Details: `Microsoft IIS 5.0 PROPFIND DoS Vulnerability (MS01-016) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.10667

. . . continues on next page . . .

... continued from previous page ...

Version used: 2023-10-10T05:05:41Z

Product Detection Result
Product: cpe:/a:microsoft:internet_information_services:5.0
Method: Microsoft Internet Information Services (IIS) Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
cve: CVE-2001-0151
url: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2001/ms01-016
url: http://www.securityfocus.com/bid/2453
url: http://support.microsoft.com/support/kb/articles/Q241/5/20.AS

Medium (CVSS: 5.0)

NVT: Microsoft IIS IDA/IDQ Path Disclosure Vulnerability - Active Check

Product detection result
cpe:/a:microsoft:internet_information_services:5.0
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)

Summary
IIS 4.0 allows a remote attacker to obtain the real pathname of the document root by requesting non-existent files with .ida or .idq extensions.

Quality of Detection: 70

Vulnerability Detection Result
Vulnerable URL: http://192.168.250.13/anything.idq

Impact
An attacker may use this flaw to gain more information about the remote host, and hence make more focused attacks.

Solution:
Solution type: Mitigation
Select 'Preferences ->Home directory ->Application', and check the checkbox 'Check if file exists' for the ISAPI mappings of your server.

Vulnerability Detection Method
Details: Microsoft IIS IDA/IDQ Path Disclosure Vulnerability - Active Check

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.10492
Version used: 2023-10-10T05:05:41Z

Product Detection Result
Product: cpe:/a:microsoft:internet_information_services:5.0
Method: Microsoft Internet Information Services (IIS) Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
cve: CVE-2000-0071
url: http://www.securityfocus.com/bid/1065

Medium (CVSS: 5.0)

NVT: Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability

Summary
Microsoft IIS Webserver is prone to IP address disclosure vulnerability.

Quality of Detection: 97

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

Impact
Successful exploitation will allow remote attackers to gain internal IP address or internal network name, which could assist in further attacks against the target host.

Solution:
Solution type: VendorFix
Apply the hotfix for IIS 6.0

Affected Software/OS
Microsoft Internet Information Services version 4.0, 5.0, 5.1 and 6.0.

Vulnerability Insight
The flaw is due to an error while processing 'GET' request. When MS IIS receives a GET request without a host header, the Web server will reveal the IP address of the server in the content-location field or the location field in the TCP header in the response.

Vulnerability Detection Method
Details: Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902796

... continues on next page ...

... continued from previous page ...

Version used: 2023-10-10T05:05:41Z

References
url: http://support.microsoft.com/kb/834141/
url: http://www.securityfocus.com/bid/3159
url: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q218180
url: http://www.juniper.net/security/auto/vulnerabilities/vuln3159.html

[return to 192.168.250.13]

2.1.13 Medium 17/tcp

Medium (CVSS: 5.0)

NVT: Check for Quote of the Day (qotd) Service (TCP)

Summary
The Quote of the Day (qotd) service is running on this host.

Quality of Detection: 80

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

Impact
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution:
Solution type: Mitigation
- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd
Then launch cmd.exe and type :
net stop simptcp
net start simptcp
To restart the service.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Check for Quote of the Day (qotd) Service (TCP)`
OID:1.3.6.1.4.1.25623.1.0.10198
Version used: `2023-08-01T13:29:10Z`

References
`cve: CVE-1999-0103`

[return to 192.168.250.13]

2.1.14 Medium 19/tcp

Medium (CVSS: 5.0)

NVT: Check for Chargen Service (TCP)

Summary
The remote host is running a 'chargen' service.

Quality of Detection: 80

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

Impact
An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution:
Solution type: Mitigation
- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen
Then launch cmd.exe and type :
net stop simptcp

... continues on next page ...

... continued from previous page ...

net start simptcp
To restart the service.

Vulnerability Insight
When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via TCP, it will continue spewing characters until the client closes the connection.
The purpose of this service was to mostly to test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third party host using this host as a relay.

Vulnerability Detection Method
Checks whether a chargen service is exposed on the target host.
Details: `Check for Chargen Service (TCP)`
OID:1.3.6.1.4.1.25623.1.0.10043
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0103`
`cve: CVE-1999-0639`

[return to 192.168.250.13]

2.1.15 Medium 7/udp

Medium (CVSS: 5.0)

NVT: echo Service Reporting (TCP + UDP)

Summary
An echo Service is running at this Host via TCP and/or UDP.

Quality of Detection: 80

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

Solution:
Solution type: Mitigation
Disable the echo Service.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The echo service is an Internet protocol defined in RFC 862. It was originally proposed for testing and measurement of round-trip times in IP networks. While still available on most UNIX-like operating systems, testing and measurement is now performed with the Internet Control Message Protocol (ICMP), using the applications ping and traceroute.

Vulnerability Detection Method
Checks whether an echo service is exposed on the target host.
Details: `echo Service Reporting (TCP + UDP)`
OID:1.3.6.1.4.1.25623.1.0.100075
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0103`
`cve: CVE-1999-0635`

[return to 192.168.250.13]

2.1.16 Medium 17/udp

Medium (CVSS: 5.0)

NVT: Check for Quote of the Day (qotd) Service (UDP)

Summary
The Quote of the Day (qotd) service is running on this host.

Quality of Detection: 80

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

Impact
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution:
Solution type: Mitigation
- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd
Then launch cmd.exe and type :
net stop simptcp

... continues on next page ...

... continued from previous page ...

net start simptcp
To restart the service.

Vulnerability Insight
A server listens for UDP datagrams on UDP port 17. When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Check for Quote of the Day (qotd) Service (UDP)`
OID:1.3.6.1.4.1.25623.1.0.108029
Version used: `2023-08-03T05:05:16Z`

References
`cve: CVE-1999-0103`

[return to 192.168.250.13]

2.1.17 Medium 137/udp

Medium (CVSS: 5.0)

NVT: Microsoft MS03-034 security check

Summary
Under certain conditions, the response to a NetBT Name Service query may, in addition to the typical reply, contain random data from the target system's memory. This data could, for example, be a segment of HTML if the user on the target system was using an Internet browser, or it could contain other types of data that exist in memory at the time that the target system responds to the NetBT Name Service query.

Quality of Detection: 99

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

Impact
An attacker could seek to exploit this vulnerability by sending a NetBT Name Service query to the target system and then examine the response to see if it included any random data from that system's memory.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Microsoft has released patches to fix this issue. Please see the references for more information.

Vulnerability Detection Method
Details: `Microsoft MS03-034 security check`
OID:1.3.6.1.4.1.25623.1.0.101015
Version used: `2023-08-01T13:29:10Z`

References
```
cve: CVE-2003-0661
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=A59CC2AC-F182-4CD5
↪-ACE7-3D4C2E3F1326&displaylang=en
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=140CF7BE-0371-4D17
↪-8F4C-951B76AC3024&displaylang=en
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=1C9D8E86-5B8C-401A
↪-88B2-4443FFB9EDC3&displaylang=en
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=378D4B58-BF2C-4406
↪-9D88-E6A3C4601795&displaylang=en
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=D0564162-4EAE-42C8
↪-B26C-E4D4D496EAD8&displaylang=en
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=F131D63A-F74F-4CAF
↪-95BD-D7FA37ADCF38&displaylang=en
url: http://www.microsoft.com/downloads/details.aspx?FamilyId=22379951-64A9-446B
↪-AC8F-3F2F080383A9&displaylang=en
```

[return to 192.168.250.13]

2.1.18 Medium 25/tcp

Medium (CVSS: 4.8)

NVT: SMTP Unencrypted Cleartext Login

Summary
The remote host is running a SMTP server that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result
```
The remote SMTP server accepts logins via the following cleartext authentication
↪ mechanisms over unencrypted connections:
LOGIN
```

... continues on next page ...

... continued from previous page ...

Impact
An attacker can uncover login names and passwords by sniffing traffic to the SMTP server.

Solution:
Solution type: Mitigation
Enable SMTPS or enforce the connection via the 'STARTTLS' command. Please see the manual of the SMTP server for more information.

Vulnerability Detection Method
Evaluates from previously collected info if a non SMTPS enabled SMTP server is providing the 'PLAIN' or 'LOGIN' authentication methods without sending the 'STARTTLS' command first.
Details: `SMTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108530
Version used: `2023-10-13T05:06:09Z`

[return to 192.168.250.13]

2.1.19 Medium 19/udp

Medium (CVSS: 5.0)

NVT: Check for Chargen Service (UDP)

Summary
The remote host is running a 'chargen' service.

Quality of Detection: 80

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

Impact
An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution:
Solution type: Mitigation
- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen
Then launch cmd.exe and type :

... continues on next page ...

... continued from previous page ...

net stop simptcp
net start simptcp
To restart the service.

Vulnerability Insight
When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet.
The purpose of this service was to mostly to test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third party host using this host as a relay.

Vulnerability Detection Method
Checks whether a chargen service is exposed on the target host.
Details: `Check for Chargen Service (UDP)`
OID:1.3.6.1.4.1.25623.1.0.108030
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0103`
`cve: CVE-1999-0639`

[return to 192.168.250.13]

2.1.20 Medium 7/tcp

Medium (CVSS: 5.0)

NVT: echo Service Reporting (TCP + UDP)

Summary
An echo Service is running at this Host via TCP and/or UDP.

Quality of Detection: 80

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

Solution:
Solution type: Mitigation
Disable the echo Service.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The echo service is an Internet protocol defined in RFC 862. It was originally proposed for testing and measurement of round-trip times in IP networks. While still available on most UNIX-like operating systems, testing and measurement is now performed with the Internet Control Message Protocol (ICMP), using the applications ping and traceroute.

Vulnerability Detection Method
Checks whether an echo service is exposed on the target host.
Details: `echo Service Reporting (TCP + UDP)`
OID:1.3.6.1.4.1.25623.1.0.100075
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0103`
`cve: CVE-1999-0635`

[return to 192.168.250.13]

2.1.21 Medium 21/tcp

Medium (CVSS: 6.4)

NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Quality of Detection: 80

Vulnerability Detection Result
```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution:
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0497`

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Anonymous access allowed, send identity (e-mail name
↪) as password.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 192.168.250.13]

2.1.22 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

... continues on next page ...

... continued from previous page ...

Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 192.168.250.13]

2.2 192.168.250.22

Host scan start Wed Apr 3 00:28:32 2024 UTC
Host scan end Wed Apr 3 01:23:09 2024 UTC

Service (Port)	Threat Level
9/tcp	High
161/udp	High
161/udp	Medium
7/udp	Medium
general/tcp	Low

2.2.1 High 9/tcp

High (CVSS: 10.0)

NVT: Check for discard Service

Summary
The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.
This service is unused these days, so it is advised that you disable it.

Quality of Detection: 80

Vulnerability Detection Result
The discard service was detected on the target host.

Solution:
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0: HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard
Then launch cmd.exe and type:
net stop simptcp
net start simptcp
To restart the service.

Vulnerability Detection Method
Checks whether a discard service is exposed on the target host.
Details: `Check for discard Service`
OID:1.3.6.1.4.1.25623.1.0.11367
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0636`

[return to 192.168.250.22]

2.2.2 High 161/udp

High (CVSS: 7.6)

NVT: Report default community names of the SNMP Agent

Summary
Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE).

Quality of Detection: 99

Vulnerability Detection Result
```
SNMP Agent responded as expected when using the following community name:
public
snmpd
```

Impact
If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.

... continues on next page ...

... continued from previous page ...

If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing network traffic, initiating processes, etc. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine.
Note that this test only gathers information and does not attempt to write to the remote device. Thus it is not possible to determine automatically whether the reported community is public or private.
Also note that information made available through a guessable community string might or might not contain sensitive data. Please review the information available through the reported community string to determine the impact of this disclosure.

Solution:
Solution type: VendorFix
Determine if the detected community string is a private community string. Determine whether a public community string exposes sensitive information. Disable the SNMP service if you don't use it or change the default community string.

Vulnerability Detection Method
Details: `Report default community names of the SNMP Agent`
OID:1.3.6.1.4.1.25623.1.0.10264
Version used: `2023-11-02T05:05:26Z`

References
`cve: CVE-1999-0472`
`cve: CVE-1999-0516`
`cve: CVE-1999-0517`
`cve: CVE-1999-0792`
`cve: CVE-2000-0147`
`cve: CVE-2001-0380`
`cve: CVE-2001-0514`
`cve: CVE-2001-1210`
`cve: CVE-2002-0109`
`cve: CVE-2002-0478`
`cve: CVE-2002-1229`
`cve: CVE-2004-1474`
`cve: CVE-2004-1775`
`cve: CVE-2004-1776`
`cve: CVE-2011-0890`
`cve: CVE-2012-4964`
`cve: CVE-2014-4862`
`cve: CVE-2014-4863`
`cve: CVE-2016-1452`
`cve: CVE-2016-5645`
`cve: CVE-2017-7922`
`cve: CVE-2020-5364`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/11237
url: http://www.securityfocus.com/bid/177
url: http://www.securityfocus.com/bid/20125
url: http://www.securityfocus.com/bid/2112
url: http://www.securityfocus.com/bid/2896
url: http://www.securityfocus.com/bid/3758
url: http://www.securityfocus.com/bid/3795
url: http://www.securityfocus.com/bid/3797
url: http://www.securityfocus.com/bid/41436
url: http://www.securityfocus.com/bid/4330
url: http://www.securityfocus.com/bid/46981
url: http://www.securityfocus.com/bid/5030
url: http://www.securityfocus.com/bid/5965
url: http://www.securityfocus.com/bid/7081
url: http://www.securityfocus.com/bid/7212
url: http://www.securityfocus.com/bid/7317
url: http://www.securityfocus.com/bid/91756
url: http://www.securityfocus.com/bid/92428
url: http://www.securityfocus.com/bid/9681
url: http://www.securityfocus.com/bid/973
url: http://www.securityfocus.com/bid/986
url: http://www.securityfocus.com/bid/99083
cert-bund: CB-K18/1132
cert-bund: CB-K16/1061
dfn-cert: DFN-CERT-2016-1130
```

[return to 192.168.250.22]

2.2.3 Medium 161/udp

Medium (CVSS: 5.0)

NVT: SNMP GETBULK Reflected DRDoS

Summary
The remote SNMP daemon allows distributed reflection and amplification (DRDoS) attacks.

Quality of Detection: 99

Vulnerability Detection Result
```
By sending an SNMP GetBulk request of 41 bytes, we received a response of 1853 b
↪ytes.
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this vulnerability allows attackers to cause denial-of-service conditions against remote hosts.

Solution:
Solution type: Workaround
Disable the SNMP service on the remote host if you do not use it or restrict access to this service.

Vulnerability Detection Method
Send an SNMP GetBulk request and check the response.
Details: `SNMP GETBULK Reflected DRDoS`
OID:1.3.6.1.4.1.25623.1.0.105062
Version used: `2023-07-27T05:05:09Z`

References
`url: http://www.darkreading.com/attacks-breaches/snmp-ddos-attacks-spike/d/d-id/`
`↪1269149`

[return to 192.168.250.22]

2.2.4 Medium 7/udp

Medium (CVSS: 5.0)

NVT: echo Service Reporting (TCP + UDP)

Summary
An echo Service is running at this Host via TCP and/or UDP.

Quality of Detection: 80

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

Solution:
Solution type: Mitigation
Disable the echo Service.

Vulnerability Insight
The echo service is an Internet protocol defined in RFC 862. It was originally proposed for testing and measurement of round-trip times in IP networks. While still available on most UNIX-like operating systems, testing and measurement is now performed with the Internet Control Message Protocol (ICMP), using the applications ping and traceroute.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks whether an echo service is exposed on the target host.
Details: `echo Service Reporting (TCP + UDP)`
OID:1.3.6.1.4.1.25623.1.0.100075
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0103`
`cve: CVE-1999-0635`

[return to 192.168.250.22]

2.2.5 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 67695619
Packet 2: 67695734
```

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

Solution:
Solution type: Mitigation
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 the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 192.168.250.22]

2.3 192.168.250.17

Host scan start Wed Apr 3 00:28:32 2024 UTC
Host scan end Wed Apr 3 01:22:39 2024 UTC

Service (Port)	Threat Level
161/udp	High
25/tcp	Medium
general/tcp	Low
general/icmp	Low

2.3.1 High 161/udp

High (CVSS: 7.6)

NVT: Report default community names of the SNMP Agent

Summary
Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE).

Quality of Detection: 99

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
SNMP Agent responded as expected when using the following community name:
all private
private
public

Impact
If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.
If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing network traffic, initiating processes, etc. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine.
Note that this test only gathers information and does not attempt to write to the remote device. Thus it is not possible to determine automatically whether the reported community is public or private.
Also note that information made available through a guessable community string might or might not contain sensitive data. Please review the information available through the reported community string to determine the impact of this disclosure.

Solution:
Solution type: VendorFix
Determine if the detected community string is a private community string. Determine whether a public community string exposes sensitive information. Disable the SNMP service if you don't use it or change the default community string.

Vulnerability Detection Method
Details: Report default community names of the SNMP Agent
OID:1.3.6.1.4.1.25623.1.0.10264
Version used: 2023-11-02T05:05:26Z

References
cve: CVE-1999-0472
cve: CVE-1999-0516
cve: CVE-1999-0517
cve: CVE-1999-0792
cve: CVE-2000-0147
cve: CVE-2001-0380
cve: CVE-2001-0514
cve: CVE-2001-1210
cve: CVE-2002-0109
cve: CVE-2002-0478
cve: CVE-2002-1229

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2004-1474
cve: CVE-2004-1775
cve: CVE-2004-1776
cve: CVE-2011-0890
cve: CVE-2012-4964
cve: CVE-2014-4862
cve: CVE-2014-4863
cve: CVE-2016-1452
cve: CVE-2016-5645
cve: CVE-2017-7922
cve: CVE-2020-5364
url: http://www.securityfocus.com/bid/11237
url: http://www.securityfocus.com/bid/177
url: http://www.securityfocus.com/bid/20125
url: http://www.securityfocus.com/bid/2112
url: http://www.securityfocus.com/bid/2896
url: http://www.securityfocus.com/bid/3758
url: http://www.securityfocus.com/bid/3795
url: http://www.securityfocus.com/bid/3797
url: http://www.securityfocus.com/bid/41436
url: http://www.securityfocus.com/bid/4330
url: http://www.securityfocus.com/bid/46981
url: http://www.securityfocus.com/bid/5030
url: http://www.securityfocus.com/bid/5965
url: http://www.securityfocus.com/bid/7081
url: http://www.securityfocus.com/bid/7212
url: http://www.securityfocus.com/bid/7317
url: http://www.securityfocus.com/bid/91756
url: http://www.securityfocus.com/bid/92428
url: http://www.securityfocus.com/bid/9681
url: http://www.securityfocus.com/bid/973
url: http://www.securityfocus.com/bid/986
url: http://www.securityfocus.com/bid/99083
cert-bund: CB-K18/1132
cert-bund: CB-K16/1061
dfn-cert: DFN-CERT-2016-1130
```

[return to 192.168.250.17]

2.3.2 Medium 25/tcp

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

... continues on next page ...

... continued from previous page ...

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Quality of Detection: 99

Vulnerability Detection Result
```
'VRFY root' produces the following answer: 250 Super-User <root@slowaris.>
'EXPN root' produces the following answer: 250 Super-User <root@slowaris.>
```

Solution:
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `2023-10-31T05:06:37Z`

References
`url: http://cr.yp.to/smtp/vrfy.html`

[return to 192.168.250.17]

2.3.3 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result
`It was detected that the host implements RFC1323/RFC7323.`

... continues on next page ...

... continued from previous page ...

```
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 54960536
Packet 2: 54960650
```

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

Solution:
Solution type: Mitigation
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 the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 192.168.250.17]

2.3.4 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

Low (CVSS: 2.1)

NVT: ICMP Netmask Reply Information Disclosure

Summary
The remote host responded to an ICMP netmask request.

Quality of Detection: 80

Vulnerability Detection Result
`Received Netmask: 255.255.254.0`

Impact
This information might give an attacker information for further reconnaissance and/or attacks (e.g. subnet structure, filter bypass, etc.).

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP netmask on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Netmask Reply is an ICMP message which replies to a Netmask message.

Vulnerability Detection Method
Details: `ICMP Netmask Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.146440
Version used: `2022-11-17T10:12:09Z`

References
`cve: CVE-1999-0524`
`url: https://www.rfc-editor.org/rfc/rfc950.html`
`url: https://www.rfc-editor.org/rfc/rfc6918.html`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.17]

2.4 192.168.250.16

Host scan start	Wed Apr 3 00:28:32 2024 UTC
Host scan end	Wed Apr 3 02:18:14 2024 UTC

Service (Port)	Threat Level
161/udp	High
520/udp	Medium
general/icmp	Low

2.4.1 High 161/udp

High (CVSS: 7.6)

NVT: Report default community names of the SNMP Agent

Summary
Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE).

Quality of Detection: 99

Vulnerability Detection Result
`SNMP Agent responded as expected when using the following community name: public`

Impact
If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.
If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing network traffic, initiating processes, etc. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine.
Note that this test only gathers information and does not attempt to write to the remote device. Thus it is not possible to determine automatically whether the reported community is public or private.
Also note that information made available through a guessable community string might or might not contain sensitive data. Please review the information available through the reported community string to determine the impact of this disclosure.

Solution:
Solution type: VendorFix
Determine if the detected community string is a private community string. Determine whether a public community string exposes sensitive information. Disable the SNMP service if you don't use it or change the default community string.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Details: Report default community names of the SNMP Agent
OID:1.3.6.1.4.1.25623.1.0.10264
Version used: 2023-11-02T05:05:26Z

References

cve: CVE-1999-0472
cve: CVE-1999-0516
cve: CVE-1999-0517
cve: CVE-1999-0792
cve: CVE-2000-0147
cve: CVE-2001-0380
cve: CVE-2001-0514
cve: CVE-2001-1210
cve: CVE-2002-0109
cve: CVE-2002-0478
cve: CVE-2002-1229
cve: CVE-2004-1474
cve: CVE-2004-1775
cve: CVE-2004-1776
cve: CVE-2011-0890
cve: CVE-2012-4964
cve: CVE-2014-4862
cve: CVE-2014-4863
cve: CVE-2016-1452
cve: CVE-2016-5645
cve: CVE-2017-7922
cve: CVE-2020-5364
url: http://www.securityfocus.com/bid/11237
url: http://www.securityfocus.com/bid/177
url: http://www.securityfocus.com/bid/20125
url: http://www.securityfocus.com/bid/2112
url: http://www.securityfocus.com/bid/2896
url: http://www.securityfocus.com/bid/3758
url: http://www.securityfocus.com/bid/3795
url: http://www.securityfocus.com/bid/3797
url: http://www.securityfocus.com/bid/41436
url: http://www.securityfocus.com/bid/4330
url: http://www.securityfocus.com/bid/46981
url: http://www.securityfocus.com/bid/5030
url: http://www.securityfocus.com/bid/5965
url: http://www.securityfocus.com/bid/7081
url: http://www.securityfocus.com/bid/7212
url: http://www.securityfocus.com/bid/7317
url: http://www.securityfocus.com/bid/91756
url: http://www.securityfocus.com/bid/92428
url: http://www.securityfocus.com/bid/9681
url: http://www.securityfocus.com/bid/973

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/986
url: http://www.securityfocus.com/bid/99083
cert-bund: CB-K18/1132
cert-bund: CB-K16/1061
dfn-cert: DFN-CERT-2016-1130
```

[return to 192.168.250.16]

2.4.2 Medium 520/udp

Medium (CVSS: 5.8)

NVT: RIP-1 Poisoning Routing Table

Summary
This host is running a RIP-1 agent.

Quality of Detection: 95

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

Impact
Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.

Solution:
Solution type: Workaround
Disable the RIP agent if you don't use it, or use RIP-2 and implement authentication.

Vulnerability Insight
RIP-1 does not implement authentication. An attacker may feed the remote host with bogus routes and hijack network connections.

Vulnerability Detection Method
Sends a RIP request and checks the response.
Details: `RIP-1 Poisoning Routing Table`
OID:1.3.6.1.4.1.25623.1.0.105236
Version used: `2022-07-08T10:11:49Z`

[return to 192.168.250.16]

2.4.3 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
`The following response / ICMP packet has been received:`
`- ICMP Type: 14`
`- ICMP Code: 0`

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.16]

2.5 192.168.250.18

Host scan start	Wed Apr 3 00:28:32 2024 UTC
Host scan end	Wed Apr 3 01:19:21 2024 UTC

Service (Port)	Threat Level
22/tcp	High
123/udp	Medium
22/tcp	Medium
22/tcp	Low
general/tcp	Low
general/icmp	Low

2.5.1 High 22/tcp

High (CVSS: 7.5)

NVT: Deprecated SSH-1 Protocol Detection

Summary
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws.

Quality of Detection: 80

Vulnerability Detection Result
```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptographic flaws:
1.33
1.5
```

Impact
Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution:
Solution type: VendorFix
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method
Details: `Deprecated SSH-1 Protocol Detection`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.801993
Version used: 2023-03-24T10:19:42Z

References
cve: CVE-2001-0361
cve: CVE-2001-0572
cve: CVE-2001-1473
url: http://www.kb.cert.org/vuls/id/684820
url: http://www.securityfocus.com/bid/2344
url: http://xforce.iss.net/xforce/xfdb/6603
cert-bund: CB-K15/1534
dfn-cert: DFN-CERT-2015-1619

[return to 192.168.250.18]

2.5.2 Medium 123/udp

Medium (CVSS: 6.4)

NVT: NTP mode 7 MODE_PRIVATE Packet Remote Denial of Service Vulnerability

Summary
NTP.org's ntpd is prone to a remote denial-of-service vulnerability because it fails to properly handle certain incoming network packets.

Quality of Detection: 99

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

Impact
An attacker can exploit this issue to cause the application to consume excessive CPU resources and fill disk space with log messages.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for details.

Vulnerability Detection Method
Send a NTP mode 7 request and check the response.
Details: NTP mode 7 MODE_PRIVATE Packet Remote Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100399
Version used: 2023-07-27T05:05:08Z

... continues on next page ...

... continued from previous page ...

References

```
cve: CVE-2009-3563
url: http://www.securityfocus.com/bid/37255
url: https://support.ntp.org/bugs/show_bug.cgi?id=1331
url: http://www.kb.cert.org/vuls/id/568372
cert-bund: WID-SEC-2024-0672
cert-bund: WID-SEC-2023-1747
dfn-cert: DFN-CERT-2012-0513
dfn-cert: DFN-CERT-2011-0487
dfn-cert: DFN-CERT-2010-1318
dfn-cert: DFN-CERT-2010-0720
dfn-cert: DFN-CERT-2010-0595
dfn-cert: DFN-CERT-2010-0425
dfn-cert: DFN-CERT-2010-0300
dfn-cert: DFN-CERT-2010-0070
dfn-cert: DFN-CERT-2010-0036
dfn-cert: DFN-CERT-2010-0025
dfn-cert: DFN-CERT-2009-1770
dfn-cert: DFN-CERT-2009-1743
dfn-cert: DFN-CERT-2009-1742
dfn-cert: DFN-CERT-2009-1741
dfn-cert: DFN-CERT-2009-1740
```

Medium (CVSS: 5.0)

NVT: NTP Monlist Feature Enabled

Summary

NTP.org's ntpd is prone to a remote denial-of-service vulnerability because it fails to properly handle certain incoming network packets.

Quality of Detection: 99

Vulnerability Detection Result

```
The Scanner was able to retrieve the following list of recent to this ntpd conne
↪cted hosts:
192.168.66.2
192.168.66.5
192.168.66.3
192.168.66.4
192.168.66.6
192.168.66.9
```

Impact

Successfully exploiting this issue may allow an attacker to cause a denial of service.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to NTP.org's ntpd 4.2.7p26 or newer or set 'disable monitor' in ntp.conf.

Affected Software/OS
NTP.org's ntpd versions before 4.2.7p26. Other implementations might be affected as well.

Vulnerability Insight
The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.

Vulnerability Detection Method
Send a NTP monlist request and check the response.
Details: `NTP Monlist Feature Enabled`
OID:1.3.6.1.4.1.25623.1.0.103868
Version used: `2023-07-14T16:09:26Z`

References
`cve: CVE-2013-5211`
`url: http://bugs.ntp.org/show_bug.cgi?id=1532`
`url: http://lists.ntp.org/pipermail/pool/2011-December/005616.html`
`cert-bund: CB-K17/1826`
`cert-bund: CB-K17/0205`
`cert-bund: CB-K14/0852`
`cert-bund: CB-K14/0291`
`cert-bund: CB-K14/0120`
`cert-bund: CB-K14/0020`
`dfn-cert: DFN-CERT-2021-0776`
`dfn-cert: DFN-CERT-2018-2593`
`dfn-cert: DFN-CERT-2017-1910`
`dfn-cert: DFN-CERT-2017-0210`
`dfn-cert: DFN-CERT-2014-0890`
`dfn-cert: DFN-CERT-2014-0303`
`dfn-cert: DFN-CERT-2014-0111`
`dfn-cert: DFN-CERT-2014-0017`

[return to 192.168.250.18]

2.5.3 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2023-10-12T05:05:32Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5
```

Medium (CVSS: 5.3)

NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-----------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2023-10-12T05:05:32Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
```

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[return to 192.168.250.18]

2.5.4 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 192.168.250.18]

2.5.5 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 784068552
Packet 2: 784069696
```

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

Solution:
Solution type: Mitigation
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.

... continues on next page ...

... continued from previous page ...

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 the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 192.168.250.18]

2.5.6 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact

... continues on next page ...

... continued from previous page ...

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.18]

2.6 192.168.250.12

Host scan start Wed Apr 3 00:28:32 2024 UTC
Host scan end Wed Apr 3 01:41:48 2024 UTC

Service (Port)	Threat Level
513/tcp	High
21/tcp	High
21/tcp	Medium
25/tcp	Medium
23/tcp	Medium
79/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
587/tcp	Medium
22/tcp	Medium
general/icmp	Low
general/tcp	Low
22/tcp	Low

2.6.1 High 513/tcp

High (CVSS: 7.5)

NVT: The rlogin service is running

Summary
This remote host is running a rlogin service.

Quality of Detection: 80

Vulnerability Detection Result
`The rlogin service is running on the target system.`

Solution:
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight
rlogin has several serious security problems,
- all information, including passwords, is transmitted unencrypted.
- .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)

Vulnerability Detection Method
Details: `The rlogin service is running`
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: `2021-09-01T07:45:06Z`

References
`cve: CVE-1999-0651`

[return to 192.168.250.12]

2.6.2 High 21/tcp

High (CVSS: 7.5)

NVT: FTP Brute Force Logins Reporting

Summary
It was possible to login into the remote FTP server using weak/known credentials.

Quality of Detection: 95

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`guest:guest`

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2023-12-06T05:06:11Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2001-1594`
`cve: CVE-2013-7404`
`cve: CVE-2017-8218`
`cve: CVE-2018-19063`

... continues on next page ...

... continued from previous page ...

cve: CVE-2018-19064

[return to 192.168.250.12]

2.6.3 Medium 21/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Guest login ok, send your complete e-mail address as
↪ password.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 192.168.250.12]

2.6.4 Medium 25/tcp

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Quality of Detection: 99

Vulnerability Detection Result
```
'VRFY root' produces the following answer: 250 2.1.5 Super-User <root@snoracle.c
↪s574.local>
'EXPN root' produces the following answer: 250 2.1.5 Super-User <root@snoracle.c
↪s574.local>
```

Solution:
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `2023-10-31T05:06:37Z`

References
`url: http://cr.yp.to/smtp/vrfy.html`

[return to 192.168.250.12]

2.6.5 Medium 23/tcp

Medium (CVSS: 4.8)

NVT: Telnet Unencrypted Cleartext Login

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

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

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution:
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[return to 192.168.250.12]

2.6.6 Medium 79/tcp

Medium (CVSS: 5.0)

NVT: Finger Service Remote Information Disclosure Vulnerability

Summary
The finger service on the remote host is prone to an information disclosure vulnerability.

Quality of Detection: 99

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

Impact
Successful exploitation will allow an attacker to obtain sensitive information that could aid in further attacks.

Solution:
Solution type: Mitigation
Disable the finger service, or install a finger service or daemon that limits the type of information provided.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS
GNU finger is known to be affected. Other finger implementations might be affected as well.

Vulnerability Insight
The flaw exists because the finger service exposes valid user information to any entity on the network.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Finger Service Remote Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.802236
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0612`
`url: http://xforce.iss.net/xforce/xfdb/46`
`url: http://www.iss.net/security_center/reference/vuln/finger-running.htm`

[return to 192.168.250.12]

2.6.7 Medium 587/tcp

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Quality of Detection: 99

Vulnerability Detection Result
```
'VRFY root' produces the following answer: 250 2.1.5 Super-User <root@snoracle.c
↪s574.local>
'EXPN root' produces the following answer: 250 2.1.5 Super-User <root@snoracle.c
↪s574.local>
```

Solution:
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.

... continues on next page ...

... continued from previous page ...

For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `2023-10-31T05:06:37Z`

References
`url: http://cr.yp.to/smtp/vrfy.html`

[return to 192.168.250.12]

2.6.8 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.

... continues on next page ...

... continued from previous page ...

Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8332`
`url: https://www.rfc-editor.org/rfc/rfc8709`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6`

Medium (CVSS: 5.3)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

... continues on next page ...

... continued from previous page ...

A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2023-10-12T05:05:32Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
arcfour
blowfish-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
arcfour
blowfish-cbc
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[return to 192.168.250.12]

2.6.9 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Netmask Reply Information Disclosure

Summary
The remote host responded to an ICMP netmask request.

Quality of Detection: 80

Vulnerability Detection Result
`Received Netmask: 255.255.254.0`

Impact

... continues on next page ...

... continued from previous page ...

This information might give an attacker information for further reconnaissance and/or attacks (e.g. subnet structure, filter bypass, etc.).

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP netmask on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Netmask Reply is an ICMP message which replies to a Netmask message.

Vulnerability Detection Method
Details: `ICMP Netmask Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.146440
Version used: `2022-11-17T10:12:09Z`

References
`cve: CVE-1999-0524`
`url: https://www.rfc-editor.org/rfc/rfc950.html`
`url: https://www.rfc-editor.org/rfc/rfc6918.html`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.12]

2.6.10 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 67596532
Packet 2: 67596646
```

... continues on next page ...

... continued from previous page ...

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

Solution:
Solution type: Mitigation
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 the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 192.168.250.12]

2.6.11 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

... continues on next page ...

... continued from previous page ...

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[return to 192.168.250.12]

2.7 192.168.250.19

Host scan start Wed Apr 3 00:28:32 2024 UTC
Host scan end Wed Apr 3 01:54:09 2024 UTC

Service (Port)	Threat Level
21/tcp	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
22/tcp	High
80/tcp	Medium
23/tcp	Medium
21/tcp	Medium
22/tcp	Medium
general/icmp	Low
21/tcp	Low
22/tcp	Low
general/tcp	Low

2.7.1 High 21/tcp

High (CVSS: 7.5)

NVT: FTP Brute Force Logins Reporting

Summary
It was possible to login into the remote FTP server using weak/known credentials.

Quality of Detection: 95

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`guest:guest`

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2023-12-06T05:06:11Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2001-1594`
`cve: CVE-2013-7404`
`cve: CVE-2017-8218`
`cve: CVE-2018-19063`
`cve: CVE-2018-19064`

[return to 192.168.250.19]

2.7.2 High 22/tcp

High (CVSS: 7.5)

NVT: Deprecated SSH-1 Protocol Detection

Summary
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws.

Quality of Detection: 80

Vulnerability Detection Result
```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptographic flaws:
1.33
1.5
```

Impact
Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution:
Solution type: VendorFix
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method
Details: `Deprecated SSH-1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: `2023-03-24T10:19:42Z`

References
`cve: CVE-2001-0361`
`cve: CVE-2001-0572`
`cve: CVE-2001-1473`
`url: http://www.kb.cert.org/vuls/id/684820`
`url: http://www.securityfocus.com/bid/2344`
`url: http://xforce.iss.net/xforce/xfdb/6603`
`cert-bund: CB-K15/1534`
`dfn-cert: DFN-CERT-2015-1619`

[return to 192.168.250.19]

2.7.3 Medium 80/tcp

Medium (CVSS: 5.8)

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Quality of Detection: 99

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

References
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 5.0)

NVT: Apache HTTP Server UserDir Sensitive Information Disclosure

Product detection result
cpe:/a:apache:http_server:1.3.23
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
An information leak occurs on Apache HTTP Server based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.

Quality of Detection: 70

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

Solution:
Solution type: Mitigation
1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'.
Or
2) Use a RedirectMatch rewrite rule under Apache – this works even if there is no such entry in the password file, e.g.: RedirectMatch ^/ (.*)$ http://example.com/$1
Or
3) Add into httpd.conf:
ErrorDocument 404 http://example.com/sample.html
ErrorDocument 403 http://example.com/sample.html
(NOTE: You need to use a FQDN inside the URL for it to work properly).

Vulnerability Detection Method
Details: Apache HTTP Server UserDir Sensitive Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.10766
Version used: 2023-06-22T10:34:15Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.23
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2001-1013
url: http://www.securiteam.com/unixfocus/5WP0C1F5FI.html

... continues on next page ...

... continued from previous page ...

url: http://www.securityfocus.com/bid/3335
cert-bund: CB-K14/0304
dfn-cert: DFN-CERT-2014-0315

Medium (CVSS: 4.3)

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Product detection result
cpe:/a:apache:http_server:1.3.23
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Quality of Detection: 99

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

Vulnerability Insight
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.23
Method: Apache HTTP Server Detection Consolidation

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.117232)

References

cve: CVE-2012-0053
url: http://secunia.com/advisories/47779
url: http://www.securityfocus.com/bid/51706
url: http://www.exploit-db.com/exploits/18442
url: http://rhn.redhat.com/errata/RHSA-2012-0128.html
url: http://httpd.apache.org/security/vulnerabilities_22.html
url: http://svn.apache.org/viewvc?view=revision&revision=1235454
url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
cert-bund: CB-K15/0080
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188

Medium (CVSS: 4.3)

NVT: Apache HTTP Server ETag Header Information Disclosure Weakness

Product detection result

cpe:/a:apache:http_server:1.3.23
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary

... continues on next page ...

... continued from previous page ...

A weakness has been discovered in the Apache HTTP Server if configured to use the FileETag directive.

Quality of Detection: 80

Vulnerability Detection Result
`Information that was gathered:`
`Inode: 20553`
`Size: 2890`

Impact
Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

Solution:
Solution type: VendorFix
OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.
Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method
Due to the way in which Apache HTTP Server generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.
Details: `Apache HTTP Server ETag Header Information Disclosure Weakness`
OID:1.3.6.1.4.1.25623.1.0.103122
Version used: `2022-12-05T10:11:03Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:1.3.23`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2003-1418`
`url: http://www.securityfocus.com/bid/6939`
`url: http://httpd.apache.org/docs/mod/core.html#fileetag`
`url: http://www.openbsd.org/errata32.html`
`url: http://support.novell.com/docs/Tids/Solutions/10090670.html`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K17/0896`
`cert-bund: CB-K15/0469`
`dfn-cert: DFN-CERT-2017-1821`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0925
dfn-cert: DFN-CERT-2015-0495
```

[return to 192.168.250.19]

2.7.4 Medium 23/tcp

Medium (CVSS: 4.8)

NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

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

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution:
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[return to 192.168.250.19]

2.7.5 Medium 21/tcp

Medium (CVSS: 6.4)

NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
total 32
d--x--x--x   2 root     root         4096 Jun 30  2016 bin
d--x--x--x   2 root     root         4096 Jun 30  2016 etc
drwxr-xr-x   2 root     root         4096 Jun 30  2016 lib
drwxr-xr-x   2 root     50           4096 Aug 22  2001 pub
Account "ftp":
total 32
d--x--x--x   2 root     root         4096 Jun 30  2016 bin
d--x--x--x   2 root     root         4096 Jun 30  2016 etc
drwxr-xr-x   2 root     root         4096 Jun 30  2016 lib
drwxr-xr-x   2 root     50           4096 Aug 22  2001 pub
```

Impact

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution:
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method

Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2021-10-20T09:03:29Z`

... continues on next page ...

... continued from previous page ...

References
cve: CVE-1999-0497

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Quality of Detection: 98

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440

... continues on next page ...

... continued from previous page ...

Version used: 2023-11-02T05:05:26Z

References

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Quality of Detection: 98

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)

... continues on next page ...

... continued from previous page ...

- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method
Check the used SSL protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2021-10-15T12:51:02Z

References
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00:C=US (Server certificate)
```

... continues on next page ...

... continued from previous page ...

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

References
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection: 99

Vulnerability Detection Result

```
The certificate of the remote service expired on 2017-06-30 21:58:49.
Certificate details:
fingerprint (SHA-1)             | D37084F7555A6304DCD0E7D3542FFEBC66FC7267
fingerprint (SHA-256)           | D6AB09899F37B54A7E085D6C6389D69EF63274BD5C361D
↪220BD7CC69CFAA3B92
issued by                       | C=US
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00
signature algorithm             | md5WithRSAEncryption
subject                         | C=US
subject alternative names (SAN) | None
valid from                      | 2016-06-30 21:58:49 UTC
```

... continues on next page ...

... continued from previous page ...

valid until	2017-06-30 21:58:49 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Guest login ok, send your complete e-mail address as
↪ password.
The remote FTP service supports the 'AUTH TLS' command but isn't enforcing the u
↪se of it for:
- Non-anonymous sessions
- Anonymous sessions
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection: 98

Vulnerability Detection Result
```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2023-10-20T16:09:12Z

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Quality of Detection: 80

Vulnerability Detection Result
`Server Temporary Key Size: 1024 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: 2023-07-21T05:05:22Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Quality of Detection: 80

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject: C=US
Signature Algorithm: md5WithRSAEncryption

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

... continues on next page ...

... continued from previous page ...

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

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

[return to 192.168.250.19]

2.7.6 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
) and SHA-1
```

Impact
An attacker can quickly break individual connections.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2023-10-12T05:05:32Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

Medium (CVSS: 5.3)

NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
----------------------------------------------------------------------------
↪---------
```

... continues on next page ...

... continued from previous page ...

ssh-dss	Digital Signature Algorithm (DSA) / Digital Signature Stand ↪ard (DSS)

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: Weak Host Key Algorithm(s) (SSH)
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: 2023-10-12T05:05:32Z

References
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption al ↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al ↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

... continues on next page ...

... continued from previous page ...

arcfour
blowfish-cbc
cast128-cbc

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: Weak Encryption Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: 2023-10-12T05:05:32Z

References
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

[return to 192.168.250.19]

2.7.7 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 192.168.250.19]

2.7.8 Low 21/tcp

Low (CVSS: 3.4)

NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

Quality of Detection: 80

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

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution:
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2023-07-26T05:05:09Z

References
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin ↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[return to 192.168.250.19]

2.7.9 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm
```

... continues on next page ...

... continued from previous page ...

↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2023-10-12T05:05:32Z

References
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 192.168.250.19]

2.7.10 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 78495649
Packet 2: 78495763

... continues on next page ...

... continued from previous page ...

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

Solution:
Solution type: Mitigation
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 the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 192.168.250.19]

2.8 192.168.250.11

Host scan start Wed Apr 3 00:28:32 2024 UTC
Host scan end Wed Apr 3 01:21:09 2024 UTC

Service (Port)	Threat Level
513/tcp	High
514/tcp	High
23/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
79/tcp	Medium
21/tcp	Medium
general/tcp	Low
general/icmp	Low

2.8.1 High 513/tcp

High (CVSS: 7.5)

NVT: The rlogin service is running

Summary
This remote host is running a rlogin service.

Quality of Detection: 80

Vulnerability Detection Result
`The rlogin service is running on the target system.`

Solution:
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight
rlogin has several serious security problems,
- all information, including passwords, is transmitted unencrypted.
- .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)

Vulnerability Detection Method
Details: `The rlogin service is running`
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: `2021-09-01T07:45:06Z`

References
`cve: CVE-1999-0651`

[return to 192.168.250.11]

2.8.2 High 514/tcp

High (CVSS: 7.5)

NVT: rsh Unencrypted Cleartext Login

Summary
This remote host is running a rsh service.

Quality of Detection: 80

Vulnerability Detection Result
`The rsh service is not allowing connections from this host.`

Solution:
Solution type: Mitigation
Disable the rsh service and use alternatives like SSH instead.

Vulnerability Insight
rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `rsh Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.100080
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0651`

[return to 192.168.250.11]

2.8.3 Medium 23/tcp

Medium (CVSS: 4.8)

NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

. . . continues on next page . . .

... continued from previous page ...

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

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution:
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[return to 192.168.250.11]

2.8.4 Medium 79/tcp

Medium (CVSS: 5.0)

NVT: Finger Service Remote Information Disclosure Vulnerability

Summary
The finger service on the remote host is prone to an information disclosure vulnerability.

Quality of Detection: 99

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

Impact
Successful exploitation will allow an attacker to obtain sensitive information that could aid in further attacks.

Solution:
Solution type: Mitigation
Disable the finger service, or install a finger service or daemon that limits the type of information provided.

Affected Software/OS
GNU finger is known to be affected. Other finger implementations might be affected as well.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw exists because the finger service exposes valid user information to any entity on the network.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Finger Service Remote Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.802236
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0612`
`url: http://xforce.iss.net/xforce/xfdb/46`
`url: http://www.iss.net/security_center/reference/vuln/finger-running.htm`

[return to 192.168.250.11]

2.8.5 Medium 21/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Guest login ok, send your complete e-mail address as
↪ password.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 192.168.250.11]

2.8.6 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 78394249
Packet 2: 78394364
```

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

Solution:
Solution type: Mitigation
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 the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 192.168.250.11]

2.8.7 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.11]

2.9 192.168.250.10

Host scan start Wed Apr 3 00:28:32 2024 UTC
Host scan end Wed Apr 3 01:12:20 2024 UTC

Service (Port)	Threat Level
22/tcp	High
22/tcp	Medium
general/icmp	Low
22/tcp	Low
general/tcp	Low

2.9.1 High 22/tcp

High (CVSS: 7.5)

NVT: Deprecated SSH-1 Protocol Detection

Summary
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws.

Quality of Detection: 80

Vulnerability Detection Result
```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptographic flaws:
1.33
1.5
```

Impact
Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution:
Solution type: VendorFix
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method
Details: `Deprecated SSH-1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: `2023-03-24T10:19:42Z`

References
```
cve: CVE-2001-0361
cve: CVE-2001-0572
cve: CVE-2001-1473
url: http://www.kb.cert.org/vuls/id/684820
url: http://www.securityfocus.com/bid/2344
url: http://xforce.iss.net/xforce/xfdb/6603
cert-bund: CB-K15/1534
dfn-cert: DFN-CERT-2015-1619
```

[return to 192.168.250.10]

2.9.2 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-----------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2023-10-12T05:05:32Z`

References
```
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
```

Medium (CVSS: 5.3)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak KEX algorithm(s):
```

. . . continues on next page . . .

... continued from previous page ...

```
KEX algorithm                          | Reason
---------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2023-10-12T05:05:32Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
rijndael128-cbc
rijndael192-cbc
rijndael256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
rijndael128-cbc
rijndael192-cbc
rijndael256-cbc
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

. . . continues on next page . . .

... continued from previous page ...

- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[return to 192.168.250.10]

2.9.3 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.10]

2.9.4 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
```

... continues on next page ...

... continued from previous page ...

```
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 192.168.250.10]

2.9.5 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection: 80

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 78234900
Packet 2: 78235016
```

... continues on next page ...

... continued from previous page ...

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

Solution:
Solution type: Mitigation
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 the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 192.168.250.10]

2.10 192.168.250.14

Host scan start	Wed Apr 3 00:28:32 2024 UTC
Host scan end	Wed Apr 3 01:16:16 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.10.1 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Netmask Reply Information Disclosure

Summary
The remote host responded to an ICMP netmask request.

Quality of Detection: 80

Vulnerability Detection Result
`Received Netmask: 255.255.255.0`

Impact
This information might give an attacker information for further reconnaissance and/or attacks (e.g. subnet structure, filter bypass, etc.).

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP netmask on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Netmask Reply is an ICMP message which replies to a Netmask message.

Vulnerability Detection Method
Details: `ICMP Netmask Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.146440
Version used: `2022-11-17T10:12:09Z`

References
`cve: CVE-1999-0524`
`url: https://www.rfc-editor.org/rfc/rfc950.html`
`url: https://www.rfc-editor.org/rfc/rfc6918.html`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
`The following response / ICMP packet has been received:`
`- ICMP Type: 14`
`- ICMP Code: 0`

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.250.14]

2.11 192.168.250.15

Host scan start	Wed Apr 3 00:28:32 2024 UTC
Host scan end	Wed Apr 3 01:12:51 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.11.1 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190

. . . continues on next page . . .

... continued from previous page ...

Version used: 2023-05-11T09:09:33Z

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

Low (CVSS: 2.1)

NVT: ICMP Netmask Reply Information Disclosure

Summary
The remote host responded to an ICMP netmask request.

Quality of Detection: 80

Vulnerability Detection Result
Received Netmask: 255.255.255.0

Impact
This information might give an attacker information for further reconnaissance and/or attacks (e.g. subnet structure, filter bypass, etc.).

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP netmask on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Netmask Reply is an ICMP message which replies to a Netmask message.

Vulnerability Detection Method
Details: ICMP Netmask Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.146440
Version used: 2022-11-17T10:12:09Z

References
cve: CVE-1999-0524
url: https://www.rfc-editor.org/rfc/rfc950.html
url: https://www.rfc-editor.org/rfc/rfc6918.html

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.250.15]
