Scan Report

March 29, 2023

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 “Windows Machine”. The scan started at Wed Mar 29 14:34:42 2023 UTC and ended at Wed Mar 29 15:13:20 2023 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
192.168.1.7	32	5	1	0	0
Total: 1	32	5	1	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 38 results selected by the filtering described above. Before filtering there were 92 results.

2 Results per Host

2.1 192.168.1.7

Host scan start	Wed Mar 29 14:36:22 2023 UTC
Host scan end	Wed Mar 29 15:13:17 2023 UTC

Service (Port)	Threat Level
9/tcp	High
general/tcp	High
445/tcp	High
135/tcp	Medium
3389/tcp	Medium
17/tcp	Medium
19/tcp	Medium
7/tcp	Medium
general/icmp	Low

2.1.1 High 9/tcp

High (CVSS: 10.0)
NVT: Check for discard Service

. . . continues on next page . . .

. . . continued from previous page . . .

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.

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 if a vulnerable version is present on the target host.
Details: `Check for discard Service`
OID:1.3.6.1.4.1.25623.1.0.11367
Version used: `2020-10-01T11:33:30Z`

References

```
cve: CVE-1999-0636
```

[return to 192.168.1.7]

2.1.2 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result

```
cpe:/o:microsoft:windows_10:1709:cb:pro
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The "Windows 10" Operating System on the remote host has reached the end of life
↪.
CPE:                 cpe:/o:microsoft:windows_10:1709:cb:pro
Installed version,
build or SP:         1709cb
EOL date:            2019-04-09
EOL info:            https://support.microsoft.com/en-US/help/13853/windows-lifecy
↪cle-fact-sheet
```

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

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: `2022-04-05T13:00:52Z`

Product Detection Result

Product: `cpe:/o:microsoft:windows_10:1709:cb:pro`

Method: `OS Detection Consolidation and Reporting`

OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.1.7]

2.1.3 High 445/tcp

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
alex:1234
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
operator:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
backup:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
asus:1234
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
nasadmin:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
nasuser:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
nas:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
User1:1234
```

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
admin:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
administrator:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Administrator:1234
```

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Admin:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
user-1:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Test:1234
```

Solution:

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
root:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
buh:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
boss:1234
```

Solution:

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
ftp:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Guest:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
User:1234
```

Solution:

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
rdp:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
rdpuser:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
rdpadmin:1234
```

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
manager:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
support:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
work:1234
```

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
netguest:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
superuser:1234
```

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
ftpadmin:1234
```

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

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
ftpuser:1234
```

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

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2022-04-11T14:03:55Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

[return to 192.168.1.7]

2.1.4 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 1536/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Endpoint: ncacn_ip_tcp:192.168.1.7[1536]
Port: 1537/tcp
     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1537]
     Annotation: Security Center
     UUID: 3473dd4d-2e88-4006-9cba-22570909dd10, version 5
     Endpoint: ncacn_ip_tcp:192.168.1.7[1537]
     Annotation: WinHttp Auto-Proxy Service
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1537]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1537]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1537]
     Annotation: Event log TCPIP
Port: 1538/tcp
     UUID: 0497b57d-2e66-424f-a0c6-157cd5d41700, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: AppInfo
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: IdSegSrv service
     UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: AppInfo
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: Proxy Manager provider server endpoint
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: IP Transition Configuration endpoint
     UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: AppInfo
     UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: AppInfo
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: IKE/Authip API
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: Adh APIs
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: Impl friendly name
     UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1538]
     Annotation: AppInfo
Port: 1539/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1539]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1539]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1539]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.7[1539]
     Annotation: KeyIso
Port: 1540/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1540]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1540]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1540]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1540]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1540]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Port: 1541/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.7[1541]
Port: 1543/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.7[1543]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution:

Solution type: Mitigation

Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: `DCE/RPC and MSRPC Services Enumeration Reporting`

OID:1.3.6.1.4.1.25623.1.0.10736

Version used: `2022-06-03T10:17:07Z`

[return to 192.168.1.7]

2.1.5 Medium 3389/tcp

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.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported 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.

. . . continues on next page . . .

. . . continued from previous page . . .

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
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: `2021-07-19T08:11:48Z`

References

```
cve: CVE-2015-0204
cve: CVE-2011-3389
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: 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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
```

[return to 192.168.1.7]

2.1.6 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.

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
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: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0103`

[return to 192.168.1.7]

2.1.7 Medium 19/tcp

Medium (CVSS: 5.0)
NVT: Check for Chargen Service (TCP)

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

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
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.
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 Chargen Service (TCP)`
OID:1.3.6.1.4.1.25623.1.0.10043
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0103`

[return to 192.168.1.7]

2.1.8 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.

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.
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: `echo Service Reporting (TCP + UDP)`
OID:1.3.6.1.4.1.25623.1.0.100075
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0635`

[return to 192.168.1.7]

2.1.9 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.1.7]

This file was automatically generated.