Scan Report

December 26, 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 "New Quick Task". The scan started at Thu Dec 26 05:45:30 2024 UTC and ended at Thu Dec 26 08:00:32 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
192.168.135.35	18	33	6	91	0
Total: 1	18	33	6	91	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 "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
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 148 results selected by the filtering described above. Before filtering there were 596 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.135.35	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.135.35

Host scan start	Thu Dec 26 05:49:04 2024 UTC
Host scan end	Thu Dec 26 08:00:21 2024 UTC

Service (Port)	Threat Level
5432/tcp	High
3632/tcp	High
514/tcp	High
6697/tcp	High
8787/tcp	High
512/tcp	High
1099/tcp	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
21/tcp	High
5900/tcp	High
6200/tcp	High
general/tcp	High
80/tcp	High
513/tcp	High
1524/tcp	High
3306/tcp	High
2121/tcp	High
5432/tcp	Medium
445/tcp	Medium
21/tcp	Medium
5900/tcp	Medium
23/tcp	Medium
22/tcp	Medium
80/tcp	Medium
2121/tcp	Medium
25/tcp	Medium
5432/tcp	Low
general/tcp	Low
22/tcp	Low
25/tcp	Low
general/icmp	Low
5432/tcp	Log
3632/tcp	Log
445/tcp	Log
514/tcp	Log
8009/tcp	Log
139/tcp	Log
6697/tcp	Log
8787/tcp	Log
512/tcp	Log
1099/tcp	Log
21/tcp	Log
111/tcp	Log
5900/tcp	Log
23/tcp	Log
53/tcp	Log
general/tcp	Log
22/tcp	Log
80/tcp	Log
513/tcp	Log
1524/tcp	Log
3306/tcp	Log

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
2121/tcp	Log
general/CPE-T	Log
25/tcp	Log

2.1.1 High 5432/tcp

High (CVSS: 9.0)

NVT: PostgreSQL Default Credentials (PostgreSQL Protocol)

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.12802
↪5)

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
It was possible to login as user postgres with password "postgres".

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

Vulnerability Detection Method
Details: PostgreSQL Default Credentials (PostgreSQL Protocol)
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: 2024-07-19T15:39:06Z

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.128025)

[return to 192.168.135.35]

2.1.2 High 3632/tcp

High (CVSS: 9.3)

NVT: DistCC RCE Vulnerability (CVE-2004-2687)

Summary
DistCC is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
`It was possible to execute the "id" command.`
`Result: uid=1(daemon) gid=1(daemon)`

Impact
DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution:
Solution type: VendorFix
Vendor updates are available. Please see the references for more information.
For more information about DistCC's security see the references.

Vulnerability Insight
DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Vulnerability Detection Method
Details: `DistCC RCE Vulnerability (CVE-2004-2687)`
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: `2022-07-07T10:16:06Z`

References
`cve: CVE-2004-2687`
`url: https://distcc.github.io/security.html`
`url: https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80`
`↪/archives/bugtraq/2005-03/0183.html`
`dfn-cert: DFN-CERT-2019-0381`

[return to 192.168.135.35]

2.1.3 High 514/tcp

High (CVSS: 7.5)

NVT: rsh Unencrypted Cleartext Login

Summary
This remote host is running a rsh service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The rsh service is misconfigured so it is allowing connections without a passwor`
`↪d or with default root:root credentials.`

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 192.168.135.35]

2.1.4 High 6697/tcp

High (CVSS: 8.1)

NVT: UnrealIRCd Authentication Spoofing Vulnerability

Product detection result
`cpe:/a:unrealircd:unrealircd:3.2.8.1`
`Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)`

... continues on next page ...

... continued from previous page ...

Summary
UnrealIRCd is prone to authentication spoofing vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 3.2.8.1`
`Fixed version: 3.2.10.7`

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

Solution:
Solution type: VendorFix
Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

Affected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `UnrealIRCd Authentication Spoofing Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.809883
Version used: `2023-07-14T16:09:27Z`

Product Detection Result
Product: `cpe:/a:unrealircd:unrealircd:3.2.8.1`
Method: `UnrealIRCd Detection`
OID: 1.3.6.1.4.1.25623.1.0.809884)

References
`cve: CVE-2016-7144`
`url: http://seclists.org/oss-sec/2016/q3/420`
`url: http://www.securityfocus.com/bid/92763`
`url: http://www.openwall.com/lists/oss-security/2016/09/05/8`
`url: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b`
`↪c50ba1a34a766`
`url: https://bugs.unrealircd.org/main_page.php`

[return to 192.168.135.35]

2.1.5 High 8787/tcp

High (CVSS: 10.0)

NVT: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities

Summary
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__se
↪nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `m
↪ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪`start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact
By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution:
Solution type: Mitigation
Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:
- Implementing taint on untrusted input
- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details: `Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: `2024-06-28T05:05:33Z`

References
`url: https://tools.cisco.com/security/center/viewAlert.x?alertId=22750`
`url: http://www.securityfocus.com/bid/47071`
`url: http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_tes`
`↪ters/`
`url: http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html`

[return to 192.168.135.35]

2.1.6 High 512/tcp

High (CVSS: 10.0)

NVT: The rexec service is running

Summary
This remote host is running a rexec service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The rexec service was detected on the target system.`

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

Vulnerability Insight
rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.
The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Method
Checks whether an rexec service is exposed on the target host.
Details: `The rexec service is running`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `2023-09-12T05:05:19Z`

... continues on next page ...

. . . continued from previous page . . .

References
cve: CVE-1999-0618

[return to 192.168.135.35]

2.1.7 High 1099/tcp

High (CVSS: 7.5)

NVT: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check

Summary
Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code (remote code execution/RCE) on a targeted system with elevated privileges.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
```
By doing an RMI request it was possible to trigger the vulnerability and make th
↪e remote host sending a request back to the scanner host (Details on the recei
↪ved packet follows).
Destination IP:   192.168.135.65 (receiving IP on scanner host side)
Destination port: 23802/tcp (receiving port on scanner host side)
Originating IP:   192.168.135.35 (originating IP from target host side)
```

Impact
An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Solution:
Solution type: Workaround
Disable class-loading. Please contact the vendor of the affected system for additional guidance.

Vulnerability Insight
The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.

Vulnerability Detection Method
Sends a crafted JRMI request and checks if the target is connecting back to the scanner host.

. . . continues on next page . . .

... continued from previous page ...

Note: For a successful detection of this flaw the target host needs to be able to reach the scanner host on a TCP port randomly generated during the runtime of the VT (currently in the range of 10000-32000).
Details: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check
OID:1.3.6.1.4.1.25623.1.0.140051
Version used: 2024-11-08T15:39:48Z

References

cve: CVE-2011-3556
url: https://web.archive.org/web/20211208040855/http://www.securitytracker.com/id?1026215
url: https://web.archive.org/web/20110824060234/http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html
url: https://tools.cisco.com/security/center/viewAlert.x?alertId=23665
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2012-0815
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1804
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

[return to 192.168.135.35]

2.1.8 High 21/tcp

High (CVSS: 9.8)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Product detection result
`cpe:/a:beasts:vsftpd:2.3.4`
`Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)`

Summary
vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution:
Solution type: VendorFix
The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method
Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `2023-12-07T05:05:41Z`

Product Detection Result
Product: `cpe:/a:beasts:vsftpd:2.3.4`
Method: `vsFTPd FTP Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.111050)

References
`cve: CVE-2011-2523`
`url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd`

. . . continues on next page . . .

... continued from previous page ...

```
↪oored.html
url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi
↪d/48539/
url: https://security.appspot.com/vsftpd.html
```

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 (QoD): 95%

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin
postgres:postgres
service:service
user:user
```

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-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways
- CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station
- CVE-2016-8731: Foscam C1 devices
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-9068: IMM2 for IBM and Lenovo System x
- CVE-2018-17771: Ingenico Telium 2 PoS terminals
- 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: `2024-12-17T05:05:41Z`

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-2014-9198`
`cve: CVE-2015-7261`
`cve: CVE-2016-8731`
`cve: CVE-2017-8218`
`cve: CVE-2018-9068`
`cve: CVE-2018-17771`
`cve: CVE-2018-19063`
`cve: CVE-2018-19064`

[return to 192.168.135.35]

2.1.9 High 5900/tcp

High (CVSS: 9.0)

NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
`It was possible to connect to the VNC server with the password: password`

Solution:
Solution type: Mitigation
Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.
Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.
Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method
Details: `VNC Brute Force Login`
OID:1.3.6.1.4.1.25623.1.0.106056
Version used: `2021-07-23T07:56:26Z`

[return to 192.168.135.35]

2.1.10 High 6200/tcp

High (CVSS: 9.8)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution:
Solution type: VendorFix
The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details: vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: 2023-12-07T05:05:41Z

References

cve: CVE-2011-2523
url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd
↪oored.html
url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi
↪d/48539/
url: https://security.appspot.com/vsftpd.html

[return to 192.168.135.35]

2.1.11 High general/tcp

High (CVSS: 10.0)

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

Product detection result

cpe:/o:canonical:ubuntu_linux:8.04
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 (QoD): 80%

Vulnerability Detection Result

The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP: 8.04
EOL date: 2013-05-09
EOL info: https://wiki.ubuntu.com/Releases

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:

... continues on next page ...

... continued from previous page ...

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

Product Detection Result
Product: `cpe:/o:canonical:ubuntu_linux:8.04`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.135.35]

2.1.12 High 80/tcp

High (CVSS: 10.0)

NVT: TWiki XSS and Command Execution Vulnerabilities

Summary
TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 01.Feb.2003
Fixed version:     4.2.4
```

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution:
Solution type: VendorFix
Upgrade to version 4.2.4 or later.

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaws are due to:
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: `TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `2024-03-01T14:37:10Z`

References
`cve: CVE-2008-5304`
`cve: CVE-2008-5305`
`url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304`
`url: http://www.securityfocus.com/bid/32668`
`url: http://www.securityfocus.com/bid/32669`
`url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305`

[return to 192.168.135.35]

2.1.13 High 513/tcp

High (CVSS: 10.0)

NVT: rlogin Passwordless Login

Summary
The rlogin service allows root access without a password.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`It was possible to gain root access without a password.`

Impact
This vulnerability allows an attacker to gain complete control over the target system.

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

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: `rlogin Passwordless Login`
OID:1.3.6.1.4.1.25623.1.0.113766
Version used: `2020-09-30T09:30:12Z`

High (CVSS: 7.5)

NVT: The rlogin service is running

Summary
This remote host is running a rlogin service.

Quality of Detection (QoD): 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 192.168.135.35]

2.1.14 High 1524/tcp

High (CVSS: 10.0)

NVT: Possible Backdoor: Ingreslock

... continues on next page ...

... continued from previous page ...

Summary
A backdoor is installed on the remote host.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
```
The service is answering to an 'id;' command with the following response: uid=0(
↪root) gid=0(root)
```

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution:
Solution type: Workaround
A whole cleanup of the infected system is recommended.

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `2023-07-25T05:05:58Z`

[return to 192.168.135.35]

2.1.15 High 3306/tcp

High (CVSS: 9.8)

NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

Product detection result
```
cpe:/a:mysql:mysql:5.0.51a
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
It was possible to login into the remote MySQL as root using weak credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
```
It was possible to login as root with an empty password.
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Mitigation
- Change the password as soon as possible
- Contact the vendor for other possible fixes / updates

Affected Software/OS
The following products are know to use such weak credentials:
- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6
- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier
- CVE-2007-6081: AdventNet EventLog Analyzer build 4030
- CVE-2009-0919: XAMPP
- CVE-2014-3419: Infoblox NetMRI before 6.8.5
- CVE-2015-4669: Xsuite 2.x
- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4
Other products might be affected as well.

Vulnerability Detection Method
Details: `MySQL / MariaDB Default Credentials (MySQL Protocol)`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `2023-11-02T05:05:26Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.0.51a`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2001-0645`
`cve: CVE-2004-2357`
`cve: CVE-2006-1451`
`cve: CVE-2007-2554`
`cve: CVE-2007-6081`
`cve: CVE-2009-0919`
`cve: CVE-2014-3419`
`cve: CVE-2015-4669`
`cve: CVE-2016-6531`
`cve: CVE-2018-15719`

[return to 192.168.135.35]

2.1.16 High 2121/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 (QoD): 95%

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`msfadmin:msfadmin`
`postgres:postgres`
`service:service`
`user:user`

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-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways
- CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station
- CVE-2016-8731: Foscam C1 devices
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-9068: IMM2 for IBM and Lenovo System x
- CVE-2018-17771: Ingenico Telium 2 PoS terminals
- 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: `2024-12-17T05:05:41Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
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-2014-9198
cve: CVE-2015-7261
cve: CVE-2016-8731
cve: CVE-2017-8218
cve: CVE-2018-9068
cve: CVE-2018-17771
cve: CVE-2018-19063
cve: CVE-2018-19064
```

[return to 192.168.135.35]

2.1.17 Medium 5432/tcp

Medium (CVSS: 5.9)

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

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary

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

Quality of Detection (QoD): 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.

... 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 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)
- 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: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

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`

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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
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
```

... continues on next page ...

... continued from previous page ...

```
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: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

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 (QoD): 98%

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
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

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

... continues on next page ...

... continued from previous page ...

```
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
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
```

... continues on next page ...

... continued from previous page ...

```
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
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: 5.3)

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 (QoD): 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:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D
↪626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C
↪omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su
↪ch thing outside US,C=XX (Server certificate)
```

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.

... continues on next page ...

... continued from previous page ...

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

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:

fingerprint (SHA-1)	ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)	E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC
issued by	1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX
public key algorithm	RSA
public key size (bits)	1024
serial	00FAF93A4C7FB6B9CC
signature algorithm	sha1WithRSAEncryption
subject	1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is

... continues on next page ...

... continued from previous page ...

```
↪ no such thing outside US,C=XX
subject alternative names (SAN) | None
valid from                      | 2010-03-17 14:07:45 UTC
valid until                     | 2010-04-16 14:07:45 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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)

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

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

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

Quality of Detection (QoD): 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

... continues on next page ...

... continued from previous page ...

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
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: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

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`

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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 (QoD): 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
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: 2024-09-30T08:38:05Z

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 (QoD): 80%

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

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)

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

. . . continues on next page . . .

... continued from previous page ...

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 192.168.135.35]

2.1.18 Medium 445/tcp

Medium (CVSS: 6.0)

NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
By sending a special crafted SMB request it was possible to execute ‘‘ping -p 5f4f70656e56415356543135303134 5f -c50 192.168.135.65‘‘ on the remote host.
Received answer (ICMP "Data" field):

```
0x00:  B9 F7 6C 67 69 36 00 00 56 54 31 35 30 31 34 5F    ..lgi6..VT15014_
0x10:  5F 4F 70 65 6E 56 41 53 56 54 31 35 30 31 34 5F    _OpenVASVT15014_
0x20:  5F 4F 70 65 6E 56 41 53 56 54 31 35 30 31 34 5F    _OpenVASVT15014_
0x30:  5F 4F 70 65 6E 56 41 53                            _OpenVAS
```

Impact
An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution:
Solution type: VendorFix
Updates are available. Please see the referenced vendor advisory.

Affected Software/OS
This issue affects Samba 3.0.0 through 3.0.25rc3.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Sends a crafted SMB request and checks if the target is connecting back to the scanner host.
Note: For a successful detection of this flaw the scanner host needs to be able to directly receive ICMP echo requests from the target.
Details: `Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.108011
Version used: `2024-11-13T05:05:39Z`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
`cve: CVE-2007-2447`
`url: http://www.securityfocus.com/bid/23972`
`url: https://www.samba.org/samba/security/CVE-2007-2447.html`

[return to 192.168.135.35]

2.1.19 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 (QoD): 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.

... continues on next page ...

... continued from previous page ...

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`

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 (QoD): 70%

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions:     331 Please specify the 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.

... 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`

[return to 192.168.135.35]

2.1.20 Medium 5900/tcp

Medium (CVSS: 4.8)

NVT: VNC Server Unencrypted Data Transmission

Summary
The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The VNC server provides the following insecure or cryptographically weak Securit
↪y Type(s):
2 (VNC authentication)
```

Impact
An attacker can uncover sensitive data by sniffing traffic to the VNC server.

Solution:
Solution type: Mitigation
Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

Vulnerability Detection Method
Details: `VNC Server Unencrypted Data Transmission`
OID:1.3.6.1.4.1.25623.1.0.108529
Version used: `2023-07-12T05:05:04Z`

References
`url: https://tools.ietf.org/html/rfc6143#page-10`

[return to 192.168.135.35]

2.1.21 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 (QoD): 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 192.168.135.35]

2.1.22 Medium 22/tcp

Medium (CVSS: 5.3)

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

Product detection result
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

. . . continues on next page . . .

... continued from previous page ...

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

Quality of Detection (QoD): 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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

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)

Product detection result
```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105565)

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)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

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

Quality of Detection (QoD): 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
arcfour128
arcfour256
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
arcfour128
```

... continues on next page ...

... continued from previous page ...

arcfour256
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
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: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

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 192.168.135.35]

2.1.23 Medium 80/tcp

Medium (CVSS: 6.8)

NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)

Summary
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.2`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution:
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later.

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details: `TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `2024-03-01T14:37:10Z`

References
`cve: CVE-2009-4898`
`url: http://www.openwall.com/lists/oss-security/2010/08/03/8`
`url: http://www.openwall.com/lists/oss-security/2010/08/02/17`
`url: http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix`
`url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki`

Medium (CVSS: 6.1)

NVT: TWiki < 6.1.0 XSS Vulnerability

... continues on next page ...

... continued from previous page ...

Summary
bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 01.Feb.2003
Fixed version:     6.1.0
```

Solution:
Solution type: VendorFix
Update to version 6.1.0 or later.

Affected Software/OS
TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `TWiki < 6.1.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141830
Version used: `2023-07-14T16:09:27Z`

References
```
cve: CVE-2018-20212
url: https://seclists.org/fulldisclosure/2019/Jan/7
url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki
```

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.135.35/mutillidae/javascript/ddsmoothmenu/jque
↪ry.min.js
```

... continues on next page ...

... continued from previous page ...

- Referenced at: http://192.168.135.35/mutillidae/

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 6.0)

NVT: TWiki CSRF Vulnerability

Summary
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.1

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution:
Solution type: VendorFix
Upgrade to version 4.3.1 or later.

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details: `TWiki CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `2024-06-28T05:05:33Z`

References
`cve: CVE-2009-1339`
`url: http://secunia.com/advisories/34880`
`url: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258`
`url: http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff`
`↪-cve-2009-1339.txt`

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 (QoD): 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:

... continues on next page ...

... continued from previous page ...

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`
`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`

... continues on next page ...

... continued from previous page ...

```
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: 5.3)

NVT: phpinfo() Output Reporting (HTTP)

Summary
Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://192.168.135.35/mutillidae/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
http://192.168.135.35/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
```

Impact
Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Solution:
Solution type: Workaround
Delete the listed files or restrict access to them.

Affected Software/OS
All systems exposing a file containing the output of the phpinfo() PHP function.

... continues on next page ...

... continued from previous page ...

This VT is also reporting if an affected endpoint for the following products have been identified:
- CVE-2008-0149: TUTOS
- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK

Vulnerability Insight
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Method
This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).
Details: `phpinfo() Output Reporting (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2024-12-17T05:05:41Z`

References
`cve: CVE-2008-0149`
`cve: CVE-2023-49282`
`cve: CVE-2023-49283`
`url: https://www.php.net/manual/en/function.phpinfo.php`

Medium (CVSS: 5.0)

NVT: /doc directory browsable

Summary
The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Vulnerable URL: http://192.168.135.35/doc/`

Solution:
Solution type: Mitigation
Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:
<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>

Vulnerability Detection Method
Details: `/doc directory browsable`
OID:1.3.6.1.4.1.25623.1.0.10056

... continues on next page ...

... continued from previous page ...

Version used: 2023-08-01T13:29:10Z

References
cve: CVE-1999-0678
url: http://www.securityfocus.com/bid/318

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following input fields were identified (URL:input name):
http://192.168.135.35/dvwa/login.php:password
http://192.168.135.35/phpMyAdmin/:pma_password
http://192.168.135.35/phpMyAdmin/?D=A:pma_password
http://192.168.135.35/tikiwiki/tiki-install.php:pass
http://192.168.135.35/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

... continues on next page ...

... continued from previous page ...

Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2023-09-07T05:05:21Z

References
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)

NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 1.3.2
Fixed version: 1.6.3
Installation
path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.135.35/mutillidae/javascript/ddsmoothmenu/jque
↪ry.min.js
- Referenced at: http://192.168.135.35/mutillidae/

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.6.3 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141637

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890

[return to 192.168.135.35]

2.1.24 Medium 2121/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 (QoD): 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 Password required for anonymous

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 192.168.135.35]

2.1.25 Medium 25/tcp

Medium (CVSS: 5.9)

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

Product detection result
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S
↪SLv3 protocols and supports one or more ciphers. Those supported ciphers can b
↪e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256
↪23.1.0.802067) 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 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)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

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: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security:1.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

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

... continues on next page ...

... continued from previous page ...

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-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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
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 (QoD): 80%

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
```

... continues on next page ...

... continued from previous page ...

↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D
↪626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C
↪omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su
↪ch thing outside US,C=XX (Server certificate)

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: 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 (QoD): 99%

Vulnerability Detection Result
'VRFY root' produces the following answer: 252 2.0.0 root

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'.

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:

fingerprint (SHA-1)	ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)	E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC
issued by	1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX
public key algorithm	RSA
public key size (bits)	1024
serial	00FAF93A4C7FB6B9CC
signature algorithm	sha1WithRSAEncryption
subject	1.2.840.113549.1.9.1=#726F6F74407562756E747538

... continues on next page ...

... continued from previous page ...

```
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
subject alternative names (SAN) | None
valid from                      | 2010-03-17 14:07:45 UTC
valid until                     | 2010-04-16 14:07:45 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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)

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

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

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

Quality of Detection (QoD): 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.
```

... continues on next page ...

... continued from previous page ...

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
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: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

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`

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.3)

NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

Impact

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution:

Solution type: VendorFix

- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS

- Hosts accepting 'RSA_EXPORT' cipher suites

... continues on next page ...

... continued from previous page ...

- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
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-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388

... continues on next page ...

... continued from previous page ...

```
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-2015-0021
```

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 (QoD): 80%

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

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)

... continues on next page ...

... continued from previous page ...

- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
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/`

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 (QoD): 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: `2024-09-30T08:38:05Z`

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

[return to 192.168.135.35]

2.1.26 Low 5432/tcp

Low (CVSS: 3.4)

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

Product detection result
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

Summary
This host is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 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

... continues on next page ...

... continued from previous page ...

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: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

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
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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 192.168.135.35]

2.1.27 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 (QoD): 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: 246799
Packet 2: 246909
```

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 192.168.135.35]

2.1.28 Low 22/tcp

Low (CVSS: 2.6)

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

Product detection result
```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

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

Quality of Detection (QoD): 80%

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

... continues on next page ...

... continued from previous page ...

```
hmac-sha1-96
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
umac-64@openssh.com
```

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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

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

[return to 192.168.135.35]

2.1.29 Low 25/tcp

Low (CVSS: 3.7)

NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

Summary
This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Impact
Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution:
Solution type: VendorFix
- Remove support for 'DHE_EXPORT' cipher suites from the service
- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

Affected Software/OS
- Hosts accepting 'DHE_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight
Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References

cve: CVE-2015-4000
url: https://weakdh.org
url: http://www.securityfocus.com/bid/74733
url: https://weakdh.org/imperfect-forward-secrecy.pdf
url: http://openwall.com/lists/oss-security/2015/05/20/8
url: https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
url: https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
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-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
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-K15/0964
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-K15/0877
cert-bund: CB-K15/0834
cert-bund: CB-K15/0802
cert-bund: CB-K15/0733
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
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-2015-1679
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-2015-1016
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-2015-0925
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0737
```

Low (CVSS: 3.4)

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

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

... continues on next page ...

... continued from previous page ...

This host is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 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: `2024-09-30T08:38:05Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

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 192.168.135.35]

2.1.30 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 (QoD): 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 192.168.135.35]

2.1.31 Log 5432/tcp

Log (CVSS: 0.0)

NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Product detection result
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25`
`↪623.1.0.103692)`

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS certificate on this port is self-signed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The certificate of the remote service is self signed.
Certificate details:
fingerprint (SHA-1)             | ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)           | E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A
↪F1E32DEE436DE813CC
issued by                       | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00FAF93A4C7FB6B9CC
signature algorithm             | sha1WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
subject alternative names (SAN) | None
valid from                      | 2010-03-17 14:07:45 UTC
valid until                     | 2010-04-16 14:07:45 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Medium Cipher Suites

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Non Weak Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
```

Solution:

Vulnerability Insight
Notes:
- As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652
↪E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complicati
↪on of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing
↪outside US,C=XX (Server certificate)
```

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-----------------------------------
```

... continues on next page ...

... continued from previous page ...

```
SSLv3           | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0         | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.1         | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2         | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.3         | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
An unknown service is running on this port.
It is usually reserved for Postgres

Solution:

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)

NVT: PostgreSQL Detection (TCP)

Summary
TCP based detection of PostgreSQL.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A PostgreSQL service has been identified on this port.`

Solution:

Log Method
The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.
Details: `PostgreSQL Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.100151
Version used: `2024-07-22T05:05:40Z`

Log (CVSS: 0.0)

NVT: SSL/TLS: PostgreSQL SSL/TLS Support Detection (PostgreSQL Protocol)

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.12802`
`↪5)`

Summary
Checks if the remote PostgreSQL server supports SSL/TLS.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote PostgreSQL server supports SSL/TLS.`

Solution:

Log Method
Details: `SSL/TLS: PostgreSQL SSL/TLS Support Detection (PostgreSQL Protocol)`
OID:1.3.6.1.4.1.25623.1.0.105013
Version used: `2024-07-24T05:06:37Z`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.128025)

References
`url: https://www.postgresql.org/docs/current/static/ssl-tcp.html`

Log (CVSS: 0.0)

NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
SSLv3
TLSv1.0
```

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)           | E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A
↪F1E32DEE436DE813CC
issued by                       | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00FAF93A4C7FB6B9CC
signature algorithm             | sha1WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
subject alternative names (SAN) | None
valid from                      | 2010-03-17 14:07:45 UTC
valid until                     | 2010-04-16 14:07:45 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

[return to 192.168.135.35]

2.1.32 Log 3632/tcp

Log (CVSS: 0.0)

NVT: DistCC Detection

Summary
Tries to detect if the remote host is running a DistCC service.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
`A DistCC service is running at this port.`

Solution:

Log Method
Details: `DistCC Detection`
OID:1.3.6.1.4.1.25623.1.0.12638
Version used: `2023-08-01T13:29:10Z`

[return to 192.168.135.35]

2.1.33 Log 445/tcp

Log (CVSS: 0.0)

NVT: SMBv1 Enabled - Active Check

Summary
The host has enabled SMBv1 for the SMB Server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`SMBv1 is enabled for the SMB Server`

Solution:

Log Method
Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:
- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).
Details: `SMBv1 Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.140151

. . . continues on next page . . .

... continued from previous page ...

Version used: 2024-01-09T05:06:46Z

References
url: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices
url: https://support.microsoft.com/en-us/kb/2696547
url: https://support.microsoft.com/en-us/kb/204279

Log (CVSS: 0.0)

NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following shares were found
IPC$

Solution:

Log Method
Details: Microsoft Windows SMB Accessible Shares
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: 2023-01-31T10:08:41Z

Log (CVSS: 0.0)

NVT: Microsoft SMB Signing Disabled

Summary
Checks if SMB Signing is disabled at the remote SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
SMB Signing is disabled at the server.

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: `Microsoft SMB Signing Disabled`
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: `2023-07-25T05:05:58Z`

Log (CVSS: 0.0)

NVT: SMB Login Successful For Authenticated Checks

Summary
It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

Quality of Detection (QoD): 80%

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

Solution:

Log Method
Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `2023-07-28T16:09:07Z`

Log (CVSS: 0.0)

NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A CIFS server is running on this port`

Solution:

Log Method
Details: `SMB/CIFS Server Detection`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.11011
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)

NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
Detected Samba
Version:       3.0.20
Location:      445/tcp
CPE:           cpe:/a:samba:samba:3.0.20
Concluded from version/product identification result:
Samba 3.0.20-Debian
Extra information:
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
```

Solution:

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2024-06-25T05:05:27Z

Log (CVSS: 0.0)

NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
Detected SMB workgroup: WORKGROUP
```

. . . continues on next page . . .

... continued from previous page ...

```
Detected SMB server: Samba 3.0.20-Debian
Detected OS: Debian GNU/Linux
```

Solution:

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2024-06-25T05:05:27Z

Log (CVSS: 0.0)

NVT: SMB log in

Summary
This script attempts to logon into the remote host using login/password credentials.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
It was possible to log into the remote host using the SMB protocol.

Solution:

Log Method
Details: SMB log in
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: 2023-11-28T05:05:32Z

Log (CVSS: 0.0)

NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Only SMBv1 is enabled on remote target

... continues on next page ...

. . . continued from previous page . . .

Solution:

Log Method
Details: `SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `2023-07-26T05:05:09Z`

[return to 192.168.135.35]

2.1.34 Log 514/tcp

Log (CVSS: 0.0)

NVT: rsh Service Detection

Summary
Checks if the remote host is running a rsh service.
Note: The reporting takes place in a separate VT 'rsh Unencrypted Cleartext Login' (OID: 1.3.6.1.4.1.25623.1.0.100080).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A rsh service is running at this port.`

Solution:

Log Method
Details: `rsh Service Detection`
OID:1.3.6.1.4.1.25623.1.0.108478
Version used: `2024-06-26T05:05:39Z`

[return to 192.168.135.35]

2.1.35 Log 8009/tcp

Log (CVSS: 0.0)

NVT: Unknown OS and Service Banner Reporting

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Nmap service detection (unknown) result for this port: ajp13
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 8009 192.168.135.35' and submit a possible collecte
↪d fingerprint to the nmap database.
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

[return to 192.168.135.35]

2.1.36 Log 139/tcp

Log (CVSS: 0.0)

NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
A SMB server is running on this port
```

. . . continues on next page . . .

... continued from previous page ...

Solution:

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: 2023-08-01T13:29:10Z

[return to 192.168.135.35]

2.1.37 Log 6697/tcp

Log (CVSS: 0.0)

NVT: IRC Server Banner Detection

Summary
This script tries to detect the banner of an IRC server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The IRC server banner is:
:irc.Metasploitable.LAN 351 FGAGACDIE Unreal3.2.8.1. irc.Metasploitable.LAN :Fhi
↪XOoE [*=2309]

Solution:

Log Method
Details: IRC Server Banner Detection
OID:1.3.6.1.4.1.25623.1.0.11156
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)

NVT: UnrealIRCd Detection

Summary
Detection of UnrealIRCd Daemon. This script sends a request to the server and gets the version from the response.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Detected UnrealIRCd
Version: 3.2.8.1
Location: 6697/tcp
CPE: cpe:/a:unrealircd:unrealircd:3.2.8.1
Concluded from version/product identification result:
Unreal3.2.8.1

Solution:

Log Method
Details: UnrealIRCd Detection
OID:1.3.6.1.4.1.25623.1.0.809884
Version used: 2022-06-01T21:00:42Z

Log (CVSS: 0.0)

NVT: Service Detection with 'GET' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
An IRC server seems to be running on this port.

Solution:

Vulnerability Insight
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Log Method
Details: Service Detection with 'GET' Request
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: 2024-09-27T05:05:23Z

[return to 192.168.135.35]

2.1.38 Log 8787/tcp

Log (CVSS: 0.0)

NVT: Service Detection with 'GET' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A Distributed Ruby (dRuby/DRb) service seems to be running on this port.`

Solution:

Vulnerability Insight
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Log Method
Details: `Service Detection with 'GET' Request`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `2024-09-27T05:05:23Z`

[return to 192.168.135.35]

2.1.39 Log 512/tcp

Log (CVSS: 0.0)

NVT: Service Detection with 'BINARY' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A rexec service seems to be running on this port.`

Solution:

Vulnerability Insight
. . . continues on next page . . .

... continued from previous page ...

This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a 'BINARY' request to the remaining unknown services and tries to identify them.

Log Method
Details: `Service Detection with 'BINARY' Request`
OID:1.3.6.1.4.1.25623.1.0.108204
Version used: `2024-12-06T05:05:38Z`

Log (CVSS: 0.0)

NVT: rexec Detection

Summary
This remote host is running a rexec service.

Quality of Detection (QoD): 80%

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

Solution:

Log Method
Details: `rexec Detection`
OID:1.3.6.1.4.1.25623.1.0.113763
Version used: `2023-07-28T16:09:07Z`

[return to 192.168.135.35]

2.1.40 Log 1099/tcp

Log (CVSS: 0.0)

NVT: RMI Registry Service Detection

Summary
Detection of a Remote Method Invocation (RMI) registry service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A RMI registry service is running at this port`

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `RMI Registry Service Detection`
OID:1.3.6.1.4.1.25623.1.0.105839
Version used: `2022-12-21T10:12:09Z`

[return to 192.168.135.35]

2.1.41 Log 21/tcp

Log (CVSS: 0.0)

NVT: vsFTPd FTP Server Detection

Summary
The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected vsFTPd
Version:       2.3.4
Location:      21/tcp
CPE:           cpe:/a:beasts:vsftpd:2.3.4
Concluded from version/product identification result:
220 (vsFTPd 2.3.4)
```

Solution:

Log Method
Details: `vsFTPd FTP Server Detection`
OID:1.3.6.1.4.1.25623.1.0.111050
Version used: `2023-07-26T05:05:09Z`

Log (CVSS: 0.0)

NVT: SSL/TLS: FTP Missing Support For AUTH TLS

... continues on next page ...

... continued from previous page ...

Summary
The remote FTP server does not support the 'AUTH TLS' command.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote FTP server does not support the 'AUTH TLS' command.`

Solution:

Log Method
Details: `SSL/TLS: FTP Missing Support For AUTH TLS`
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: `2021-03-19T08:13:38Z`

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 2.3.4)
```

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)

NVT: FTP Banner Detection

Summary
This script detects and reports a FTP Server Banner.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Remote FTP server banner:
220 (vsFTPd 2.3.4)
This is probably (a):
- vsFTPd
Server operating system information collected via "SYST" command:
215 UNIX Type: L8
Server status information collected via "STAT" command:
211-FTP server status:
     Connected to 192.168.135.65
     Logged in as ftp
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     vsFTPd 2.3.4 - secure, fast, stable
211 End of status
```

Solution:

Log Method
Details: FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: 2024-06-07T15:38:39Z

[return to 192.168.135.35]

2.1.42 Log 111/tcp

Log (CVSS: 0.0)

NVT: RPC Portmapper Service Detection (TCP)

Summary

. . . continues on next page . . .

... continued from previous page ...

TCP based detection of a RPC portmapper service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected RPC Portmapper
Location:      111/tcp
CPE:           cpe:/a:portmap:portmap
Extra information:
Possible known aliases / names for this product are 'port mapper', 'rpc.portmap'
↪, 'portmap' or 'rpcbind'
```

Solution:

Vulnerability Insight

The RPC portmapper service is an unsecured protocol for Internet facing systems and should only be used on a trusted network segment, otherwise disabled. The software should be patched and configured properly.

Log Method

Details: `RPC Portmapper Service Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108090
Version used: `2023-09-12T05:05:19Z`

References

```
cve: CVE-1999-0632
url: https://en.wikipedia.org/wiki/Portmap
url: https://datatracker.ietf.org/doc/html/rfc1833
```

Log (CVSS: 0.0)

NVT: Obtain list of all port mapper registered programs via RPC

Summary

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
These are the registered RPC programs:
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP
```

... continues on next page ...

... continued from previous page ...

```
RPC program #100024 version 1 'status' on port 38083/TCP
RPC program #100005 version 1 'mountd' (mount showmount) on port 43746/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 43746/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 43746/TCP
RPC program #100021 version 1 'nlockmgr' on port 51018/TCP
RPC program #100021 version 3 'nlockmgr' on port 51018/TCP
RPC program #100021 version 4 'nlockmgr' on port 51018/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 35133/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 35133/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 35133/UDP
RPC program #100021 version 1 'nlockmgr' on port 42995/UDP
RPC program #100021 version 3 'nlockmgr' on port 42995/UDP
RPC program #100021 version 4 'nlockmgr' on port 42995/UDP
RPC program #100024 version 1 'status' on port 46078/UDP
```

Solution:

Log Method
Details: `Obtain list of all port mapper registered programs via RPC`
OID:1.3.6.1.4.1.25623.1.0.11111
Version used: `2023-09-08T05:06:21Z`

[return to 192.168.135.35]

2.1.43 Log 5900/tcp

Log (CVSS: 0.0)

NVT: VNC Server and Protocol Version Detection

Summary
The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.
This allows authenticated users of the remote host to take its control remotely.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A VNC server seems to be running on this port.`

... continues on next page ...

... continued from previous page ...

The version of the VNC protocol is : RFB 003.003

Solution:
Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method
Details: VNC Server and Protocol Version Detection
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)

NVT: VNC Supported 'security types' Detection (Remote)

Summary
This script checks the remote VNC protocol version and the available 'security types'.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
The remote VNC server chose security type #2 (VNC authentication)

Solution:

Log Method
Details: VNC Supported 'security types' Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: 2023-07-12T05:05:05Z

[return to 192.168.135.35]

2.1.44 Log 23/tcp

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A telnet server seems to be running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)

NVT: Telnet Service Detection

Summary
This scripts tries to detect a Telnet service running at the remote host.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A Telnet server seems to be running on this port`

Solution:

Log Method
Details: `Telnet Service Detection`
OID:1.3.6.1.4.1.25623.1.0.100074
Version used: `2023-07-28T16:09:08Z`

References
`url: https://tools.ietf.org/html/rfc854`

Log (CVSS: 0.0)

NVT: Telnet Banner Reporting

Summary
This scripts reports the received banner of a Telnet service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Remote Telnet banner:
                                _                  _       _ _        _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
```

Solution:

Log Method
Details: Telnet Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: 2024-09-27T05:05:23Z

[return to 192.168.135.35]

2.1.45 Log 53/tcp

Log (CVSS: 0.0)

NVT: DNS Server Detection (TCP)

Summary
TCP based detection of a DNS server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote DNS server banner is:
```

. . . continues on next page . . .

... continued from previous page ...

9.4.2

Solution:

Log Method
Details: DNS Server Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: 2021-11-30T08:05:58Z

[return to 192.168.135.35]

2.1.46 Log general/tcp

Log (CVSS: 0.0)

NVT: jQuery Detection Consolidation

Summary
Consolidation of jQuery detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected jQuery
Version:       1.3.2
Location:      /mutillidae/javascript/ddsmoothmenu/jquery.min.js
CPE:           cpe:/a:jquery:jquery:1.3.2
Concluded from version/product identification result:
src="./javascript/ddsmoothmenu/jquery.min.js
jQuery JavaScript Library v1.3.2
Concluded from version/product identification location:
- Identified file: http://192.168.135.35/mutillidae/javascript/ddsmoothmenu/jque
↪ry.min.js
- Referenced at:   http://192.168.135.35/mutillidae/
```

Solution:

Log Method
Details: jQuery Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.150658
Version used: 2023-07-14T05:06:08Z

References

... continues on next page ...

... continued from previous page ...

url: https://jquery.com/

Log (CVSS: 0.0)

NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The scanner cannot reach any of the previously open ports of the remote host at the end of its scan.
This might be an availability problem related which might be due to the following reasons :
- The remote host is now down, either because a user turned it off during the scan
- A network outage has been experienced during the scan, and the remote network cannot be reached from the scanner server any more
- The scanner has been blacklisted by the system administrator or by automatic intrusion detection/prevention systems which have detected the vulnerability assessment.
In any case, the audit of the remote host might be incomplete and may need to be done again

Solution:

Log Method
Details: Check open ports
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: 2023-08-03T05:05:16Z

Log (CVSS: 0.0)

NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Hostname determination for IP 192.168.135.35:
Hostname|Source
192.168.135.35|IP-address
```

Solution:

Log Method
Details: Hostname Determination Reporting
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2022-07-27T10:11:28Z

Log (CVSS: 0.0)

NVT: PostgreSQL Detection Consolidation

Summary
Consolidation of PostgreSQL detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected PostgreSQL
Version:       8.3.1
Location:      5432/tcp
CPE:           cpe:/a:postgresql:postgresql:8.3.1
Concluded from version/product identification result:
select version(); query result: T versionDg]PostgreSQL 8.3.1 on i486-pc-linux-gn
↪u, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)CSELECTZI
```

Solution:

Log Method
Details: PostgreSQL Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.128025
Version used: 2024-07-19T05:05:32Z

References
url: https://www.postgresql.org/

Log (CVSS: 0.0)

NVT: ISC BIND Detection Consolidation

Summary
Consolidation of ISC BIND detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected ISC BIND
Version:       9.4.2
Location:      53/tcp
CPE:           cpe:/a:isc:bind:9.4.2
Concluded from version/product identification result:
9.4.2
```

Solution:

Log Method
Details: `ISC BIND Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.145294
Version used: `2022-03-28T10:48:38Z`

References
`url: https://www.isc.org/bind/`

Log (CVSS: 0.0)

NVT: OpenSSH Detection Consolidation

Summary
Consolidation of OpenSSH detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected OpenSSH Server
Version:       4.7p1
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:4.7p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: OpenSSH Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: 2024-12-13T05:05:32Z

References
url: https://www.openssh.com/

Log (CVSS: 0.0)

NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Best matching OS:
OS:           Ubuntu 8.04
Version:      8.04
CPE:          cpe:/o:canonical:ubuntu_linux:8.04
Found by VT:  1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH
↪ Banner))
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:           Linux/Unix
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.105355 (Operating System (OS) Detection (FTP
↪))
Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 2.3.4)
OS:           Debian GNU/Linux
CPE:          cpe:/o:debian:debian_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.105355 (Operating System (OS) Detection (FTP
↪))
Concluded from FTP banner on port 2121/tcp: 220 ProFTPD 1.3.1 Server (Debian) [:
↪:ffff:192.168.135.35]
OS:           Debian GNU/Linux
```

... continues on next page ...

... continued from previous page ...

```
CPE:           cpe:/o:debian:debian_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp:
OS String:  Unix
SMB String: Samba 3.0.20-Debian
OS:            Ubuntu 8.04
Version:       8.04
CPE:           cpe:/o:canonical:ubuntu_linux:8.04
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from PHP Server banner on port 80/tcp: X-Powered-By: PHP/5.2.4-2ubuntu
↪5.10
OS:            Ubuntu 8.04
Version:       8.04
CPE:           cpe:/o:canonical:ubuntu_linux:8.04
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.2.8 (Ubuntu)
↪DAV/2
OS:            Ubuntu
CPE:           cpe:/o:canonical:ubuntu_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.111068 (Operating System (OS) Detection (SMT
↪P/POP3/IMAP))
Concluded from SMTP banner on port 25/tcp: 220 metasploitable.localdomain ESMTP
↪Postfix (Ubuntu)
OS:            Ubuntu 8.04
Version:       8.04
CPE:           cpe:/o:canonical:ubuntu_linux:8.04
Found by VT:  1.3.6.1.4.1.25623.1.0.111069 (Operating System (OS) Detection (Tel
↪net))
Concluded from Telnet banner on port 23/tcp:                  _
↪_       _ _         _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
OS:            Ubuntu
CPE:           cpe:/o:canonical:ubuntu_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.108192 (Operating System (OS) Detection (MyS
↪QL/MariaDB))
Concluded from MySQL/MariaDB server banner on port 3306/tcp: 5.0.51a-3ubuntu5
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2024-12-24T05:05:31Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)

NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
`The following additional but not resolvable hostnames were detected:`
`ubuntu804-base.localdomain`

Solution:

Log Method
Details: `SSL/TLS: Hostname discovery from server certificate`
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: `2021-11-22T15:32:39Z`

Log (CVSS: 0.0)

NVT: Apache HTTP Server Detection Consolidation

Summary
Consolidation of Apache HTTP Server detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Detected Apache HTTP Server`

... continues on next page ...

... continued from previous page ...

```
Version:       2.2.8
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.2.8
Concluded from version/product identification result:
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

Solution:

Log Method
Details: Apache HTTP Server Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.117232
Version used: 2024-03-08T15:37:10Z

References
url: https://httpd.apache.org

Log (CVSS: 0.0)

NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (192.168.135.65) to target (192.168.135.35):
192.168.135.65
192.168.135.35
Network distance between scanner and target: 2
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: 2022-10-17T11:13:19Z

[return to 192.168.135.35]

2.1.47 Log 22/tcp

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`An ssh server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)

NVT: SSH Server type and version

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Remote SSH server banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Remote SSH supported authentication: none,password,publickey,hostbased,keyboard-
↪interactive
Remote SSH text/login banner: (not available)
This is probably:
```

. . . continues on next page . . .

... continued from previous page ...

```
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVASVT
Password: OpenVASVT
```

Solution:

Vulnerability Insight
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2024-08-02T05:05:39Z`

Log (CVSS: 0.0)

NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms are supported by the remote SSH service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following options are supported by the remote SSH service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
encryption_algorithms_server_to_client:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server:
```

... continues on next page ...

... continued from previous page ...

```
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Solution:

Log Method
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `2024-06-17T08:31:37Z`

Log (CVSS: 0.0)

NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
```

Solution:

Log Method
The following versions are tried: 1.33, 1.5, 1.99 and 2.0.
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `2024-06-17T08:31:37Z`

[return to 192.168.135.35]

2.1.48 Log 80/tcp

Log (CVSS: 0.0)

NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                        | Enumeration technique
------------------------------------------------------------------------------
↪----------------------
Server: Apache/2.2.8 (Ubuntu) DAV/2 | Invalid HTTP 00.5 GET request (non-existen
↪t HTTP version) to '/'
X-Powered-By: PHP/5.2.4-2ubuntu5.10 | Invalid HTTP 00.5 GET request (non-existen
↪t HTTP version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)

NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

Solution:

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)

NVT: 'favicon.ico' Based Fingerprinting (HTTP)

Summary
HTTP based fingerprinting of web applications based on an exposed 'favicon.ico' file.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following apps/services were identified:
"phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://192.168.135.3
↪5/phpMyAdmin/favicon.ico"
```

Solution:

Log Method
Details: 'favicon.ico' Based Fingerprinting (HTTP)
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)

NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Missing Headers                   | More Information
-----------------------------------------------------------------------------
↪-----------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
```

... continues on next page ...

... continued from previous page ...

```
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/

... continues on next page ...

... continued from previous page ...

```
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/
```

Log (CVSS: 0.0)

NVT: TWiki Version Detection

Summary
Detection of TWiki.
The script sends a HTTP connection request to the server and attempts to detect the presence of TWiki and to extract its version.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected TWiki
Version:       01.Feb.2003
Location:      /twiki/bin
CPE:           cpe:/a:twiki:twiki:01.Feb.2003
Concluded from version/product identification result:
This site is running TWiki version <strong>01 Feb 2003</strong>
```

Solution:

Log Method
Details: `TWiki Version Detection`
OID:1.3.6.1.4.1.25623.1.0.800399
Version used: `2023-07-25T05:05:58Z`

Log (CVSS: 0.0)

NVT: Web Application Scanning Consolidation / Info Reporting

Summary
The script consolidates and reports various information for web application (formerly called 'CGI') scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

... continues on next page ...

... continued from previous page ...

- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "192.168.135.35" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 23.13.1)" was used to acces
↪s the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
A possible recursion was detected during web application scanning:
The service is using a relative URL in one or more HTML references where e.g. /f
↪ile1.html contains <a href="subdir/file2.html"> and a subsequent request for s
↪ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi
↪r/subdir/file2.html causing a recursion. To work around this counter-measures
↪have been enabled but the service should be fixed as well to not use such prob
↪lematic links. Below an excerpt of URLs is shown to help identify those issues
↪.
Syntax : URL (HTML link)
http://192.168.135.35/mutillidae/index.php (index.php?page=documentation/how-to-
↪access-Mutillidae-over-Virtual-Box-network.php)
http://192.168.135.35/mutillidae/index.php (index.php?page=documentation/vulnera
↪bilities.php)
The following directories were used for web application scanning:
http://192.168.135.35/
http://192.168.135.35/cgi-bin
http://192.168.135.35/dav
http://192.168.135.35/doc
http://192.168.135.35/dvwa
http://192.168.135.35/index
http://192.168.135.35/index/ajax
http://192.168.135.35/mutillidae
http://192.168.135.35/mutillidae/documentation
http://192.168.135.35/oops/TWiki
http://192.168.135.35/phpMyAdmin
http://192.168.135.35/rdiff/TWiki
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.135.35/test
http://192.168.135.35/test/testoutput
http://192.168.135.35/tikiwiki
http://192.168.135.35/tikiwiki/lib
http://192.168.135.35/twiki
http://192.168.135.35/twiki/pub
http://192.168.135.35/twiki/pub/TWiki/FileAttachment
http://192.168.135.35/twiki/pub/TWiki/TWikiDocGraphics
http://192.168.135.35/twiki/pub/TWiki/TWikiLogos
http://192.168.135.35/twiki/pub/TWiki/TWikiPreferences
http://192.168.135.35/twiki/pub/TWiki/TWikiTemplates
http://192.168.135.35/twiki/pub/icn
http://192.168.135.35/view/TWiki
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
http://192.168.135.35/dvwa/dvwa/css
http://192.168.135.35/dvwa/dvwa/images
http://192.168.135.35/icons
http://192.168.135.35/index.php/installer
http://192.168.135.35/index.php/s
http://192.168.135.35/index.php/wp-json
http://192.168.135.35/mutillidae/images
http://192.168.135.35/mutillidae/javascript
http://192.168.135.35/mutillidae/javascript/ddsmoothmenu
http://192.168.135.35/mutillidae/styles
http://192.168.135.35/mutillidae/styles/ddsmoothmenu
http://192.168.135.35/phpMyAdmin/themes/original/img
http://192.168.135.35/tikiwiki/img/icons
http://192.168.135.35/tikiwiki/styles
http://192.168.135.35/tikiwiki/styles/transitions
Directory index found at:
http://192.168.135.35/dav/
http://192.168.135.35/mutillidae/documentation/
http://192.168.135.35/test/
http://192.168.135.35/test/testoutput/
http://192.168.135.35/twiki/TWikiDocumentation.html
http://192.168.135.35/twiki/bin/view/TWiki/TWikiDocumentation
http://192.168.135.35/twiki/bin/view/TWiki/TWikiInstallationGuide
Extraneous phpinfo() output found at:
http://192.168.135.35/mutillidae/phpinfo.php
Concluded from:
```

... continues on next page ...

... continued from previous page ...

```
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
http://192.168.135.35/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
PHP script discloses physical path at:
http://192.168.135.35/mutillidae/documentation/vulnerabilities.php (/var/www/mut
↪illidae/documentation/vulnerabilities.php)
http://192.168.135.35/tikiwiki/tiki-install.php (/var/www/tikiwiki/lib/adodb/dri
↪vers/adodb-mysql.inc.php)
The "Number of pages to mirror" setting (Current: 200) of the VT "Web mirroring"
↪ (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to
↪mirror this host more thoroughly but might increase the scanning time.
NOTE: The 'Maximum number of items shown for each list' setting has been reached
↪. There are 355 additional entries available for the following truncated list.
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://192.168.135.35/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://192.168.135.35/dvwa/login.php (username [] password [] Login [Login] )
http://192.168.135.35/mutillidae/ (page [add-to-your-blog.php] )
http://192.168.135.35/mutillidae/documentation/ (C=S;O [A] C=N;O [D] C=M;O [A] C
↪=D;O [A] )
http://192.168.135.35/mutillidae/index.php (username [anonymous] do [toggle-hint
↪s] page [home.php] )
http://192.168.135.35/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10]
↪)
http://192.168.135.35/phpMyAdmin/index.php (phpMyAdmin [583c9d08a7e6b1a2c44dc993
↪450927e77a819b0f] token [***replaced***] pma_username [] table [] lang [] serv
↪er [1] db [] convcharset [utf-8] pma_password [] )
http://192.168.135.35/phpMyAdmin/phpmyadmin.css.php (token [***replaced***] js_f
↪rame [right] lang [en-utf-8] nocache [2457687151] convcharset [utf-8] )
http://192.168.135.35/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
http://192.168.135.35/test/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://192.168.135.35/test/testoutput/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A]
↪)
http://192.168.135.35/tikiwiki/tiki-install.php (host [localhost] dbinfo [] pass
↪ [] name [] db [] restart [1] resetdb [] user [] )
http://192.168.135.35/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.tx
↪t] revInfo [1] )
http://192.168.135.35/twiki/bin/edit/Know/ReadmeFirst (t [1735193800] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.135.35/twiki/bin/edit/Know/WebChanges (t [1735193629] )
http://192.168.135.35/twiki/bin/edit/Know/WebHome (t [1735193590] )
http://192.168.135.35/twiki/bin/edit/Know/WebIndex (t [1735193802] )
http://192.168.135.35/twiki/bin/edit/Know/WebNotify (t [1735193805] )
http://192.168.135.35/twiki/bin/edit/Know/WebPreferences (t [1735193636] )
http://192.168.135.35/twiki/bin/edit/Know/WebSearch (t [1735193634] )
http://192.168.135.35/twiki/bin/edit/Know/WebStatistics (t [1735193807] )
http://192.168.135.35/twiki/bin/edit/Know/WebTopicList (t [1735193804] )
http://192.168.135.35/twiki/bin/edit/Main/BillClinton (topicparent [Main.TWikiUs
↪ers] )
http://192.168.135.35/twiki/bin/edit/Main/CharleytheHorse (t [1735193820] )
http://192.168.135.35/twiki/bin/edit/Main/ChristopheVermeulen (topicparent [Main
↪.TWikiUsers] )
http://192.168.135.35/twiki/bin/edit/Main/DavidWarman (topicparent [Main.TWikiUs
↪ers] )
http://192.168.135.35/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TW
↪ikiGroups] )
http://192.168.135.35/twiki/bin/edit/Main/GoodStyle (topicparent [Main.WebHome]
↪)
http://192.168.135.35/twiki/bin/edit/Main/JohnAltstadt (topicparent [Main.TWikiU
↪sers] )
http://192.168.135.35/twiki/bin/edit/Main/JohnTalintyre (t [1735193821] )
http://192.168.135.35/twiki/bin/edit/Main/MartinRaabe (topicparent [TWiki.TWikiU
↪pgradeGuide] )
http://192.168.135.35/twiki/bin/edit/Main/NicholasLee (t [1735193822] )
http://192.168.135.35/twiki/bin/edit/Main/OfficeLocations (t [1735193599] )
http://192.168.135.35/twiki/bin/edit/Main/PeterFokkinga (topicparent [Main.TWiki
↪Users] )
http://192.168.135.35/twiki/bin/edit/Main/PeterThoeny (t [1735193703] )
http://192.168.135.35/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiG
↪roups] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiAdminGroup (t [1735193827] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiGroups (t [1735193597] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiGuest (t [1735193823] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiPreferences (topicparent [Main.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiRegistration (topicparent [Main.T
↪WikiUsers] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiUsers (t [1735193596] )
http://192.168.135.35/twiki/bin/edit/Main/TWikiWeb (topicparent [Main.WebHome] )
http://192.168.135.35/twiki/bin/edit/Main/TestArea (topicparent [Main.WebHome] )
http://192.168.135.35/twiki/bin/edit/Main/TextFormattingFAQ (topicparent [Main.W
↪ebHome] )
http://192.168.135.35/twiki/bin/edit/Main/TextFormattingRules (topicparent [Main
↪.WebHome] )
http://192.168.135.35/twiki/bin/edit/Main/WebChanges (t [1735193601] )
http://192.168.135.35/twiki/bin/edit/Main/WebHome (t [1735193578] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.135.35/twiki/bin/edit/Main/WebIndex (t [1735193606] )
http://192.168.135.35/twiki/bin/edit/Main/WebNotify (t [1735193642] )
http://192.168.135.35/twiki/bin/edit/Main/WebPreferences (t [1735193610] )
http://192.168.135.35/twiki/bin/edit/Main/WebSearch (t [1735193607] )
http://192.168.135.35/twiki/bin/edit/Main/WebStatistics (t [1735193643] )
http://192.168.135.35/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Mai
↪n.WebPreferences] )
http://192.168.135.35/twiki/bin/edit/Main/WebTopicList (t [1735193641] )
http://192.168.135.35/twiki/bin/edit/Main/WelcomeGuest (topicparent [Main.WebHom
↪e] )
http://192.168.135.35/twiki/bin/edit/Main/WikiName (topicparent [Main.TWikiUsers
↪] )
http://192.168.135.35/twiki/bin/edit/Main/WikiNotation (topicparent [Main.TWikiU
↪sers] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.We
↪bHome] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebChanges (t [1735193637] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebHome (t [1735193592] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebIndex (t [1735193810] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebNotify (t [1735193816] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebPreferences (t [1735193640] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebSearch (t [1735193639] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebStatistics (t [1735193817] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent [
↪Sandbox.WebPreferences] )
http://192.168.135.35/twiki/bin/edit/Sandbox/WebTopicList (t [1735193815] )
http://192.168.135.35/twiki/bin/edit/TWiki/ (topic [] topicparent [TWikiFAQ] onl
↪ywikiname [on] templatetopic [TWikiFaqTemplate] )
http://192.168.135.35/twiki/bin/edit/TWiki/AppendixFileSystem (t [1735193783] )
http://192.168.135.35/twiki/bin/edit/TWiki/BumpyWord (t [1735193831] )
http://192.168.135.35/twiki/bin/edit/TWiki/DefaultPlugin (t [1735193731] )
http://192.168.135.35/twiki/bin/edit/TWiki/FileAttachment (t [1735193725] )
http://192.168.135.35/twiki/bin/edit/TWiki/FormattedSearch (t [1735193762] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.135.35/twiki/bin/edit/TWiki/GnuGeneralPublicLicense (t [173519379
↪0] )
http://192.168.135.35/twiki/bin/edit/TWiki/GoodStyle (t [1735193691] )
http://192.168.135.35/twiki/bin/edit/TWiki/InstalledPlugins (t [1735193788] )
http://192.168.135.35/twiki/bin/edit/TWiki/InstantEnhancements (t [1735193738] )
http://192.168.135.35/twiki/bin/edit/TWiki/InterWikis (t [1735193734] )
http://192.168.135.35/twiki/bin/edit/TWiki/InterwikiPlugin (t [1735193732] )
http://192.168.135.35/twiki/bin/edit/TWiki/ManagingTopics (t [1735193779] )
http://192.168.135.35/twiki/bin/edit/TWiki/ManagingWebs (t [1735193782] )
http://192.168.135.35/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.T
↪extFormattingFAQ] )
http://192.168.135.35/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiSho
↪rthand] )
http://192.168.135.35/twiki/bin/edit/TWiki/NotExistingYet (topicparent [TWiki.Te
↪xtFormattingRules] )
http://192.168.135.35/twiki/bin/edit/TWiki/PeterThoeny (t [1735193789] )
http://192.168.135.35/twiki/bin/edit/TWiki/SiteMap (t [1735193789] )
http://192.168.135.35/twiki/bin/edit/TWiki/StartingPoints (t [1735193613] )
http://192.168.135.35/twiki/bin/edit/TWiki/TWikiAccessControl (t [1735193753] )
http://192.168.135.35/twiki/bin/edit/TWiki/TWikiAdminCookBook (t [1735193735] )
http://192.168.135.35/twiki/bin/edit/TWiki/TWikiCourseOutlineExample (topicparen
↪t [TWiki.WebHome] )
http://192.168.135.35/twiki/bin/edit/TWiki/TWikiFAQ (t [1735193647] )
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

A web server is running on this port

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)

NVT: PHP Detection (HTTP)

Summary
HTTP based detection of PHP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected PHP
Version:       5.2.4
Location:      80/tcp
CPE:           cpe:/a:php:php:5.2.4
Concluded from version/product identification result:
X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

Solution:

Log Method
Details: PHP Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: 2024-06-12T05:05:44Z

Log (CVSS: 0.0)

NVT: phpMyAdmin Detection (HTTP)

... continues on next page ...

... continued from previous page ...

Summary
HTTP based detection of phpMyAdmin.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected phpMyAdmin
Version:       3.1.1
Location:      /phpMyAdmin
CPE:           cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Concluded from version/product identification result:
Version 3.1.1
Concluded from version/product identification location:
  http://192.168.135.35/phpMyAdmin/index.php
  http://192.168.135.35/phpMyAdmin/README
Extra information:
- Protected by Username/Password
```

Solution:

Log Method
Details: `phpMyAdmin Detection (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: `2024-02-19T14:37:31Z`

[return to 192.168.135.35]

2.1.49 Log 513/tcp

Log (CVSS: 0.0)

NVT: Service Detection with 'BINARY' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
A rlogin service seems to be running on this port.
```

Solution:

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a 'BINARY' request to the remaining unknown services and tries to identify them.

Log Method
Details: `Service Detection with 'BINARY' Request`
OID:1.3.6.1.4.1.25623.1.0.108204
Version used: `2024-12-06T05:05:38Z`

[return to 192.168.135.35]

2.1.50 Log 1524/tcp

Log (CVSS: 0.0)

NVT: Service Detection with 'GET' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`A root shell of Metasploitable seems to be running on this port.`

Solution:

Vulnerability Insight
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Log Method
Details: `Service Detection with 'GET' Request`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `2024-09-27T05:05:23Z`

[return to 192.168.135.35]

2.1.51 Log 3306/tcp

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`An unknown service is running on this port.`
`It is usually reserved for MySQL`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)

NVT: Database Open Access Information Disclosure Vulnerability

Summary
Various Database server might be prone to an information disclosure vulnerability if accessible to remote systems.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Oracle MySQL can be accessed by remote attackers`

Impact
Successful exploitation could allow an attacker to obtain sensitive information from the database.

Solution:
Solution type: Workaround
Restrict database access to remote systems. Please see the manual of the affected database server for more information.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS
- Oracle MySQL
- MariaDB
- IBM DB2
- PostgreSQL
- IBM solidDB
- Oracle Database
- Microsoft SQL Server

Vulnerability Insight
The remote database server is not restricting direct access from remote systems.

Log Method
Checks the result of various database server detections and evaluates their results.
Details: `Database Open Access Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902799
Version used: `2024-07-19T15:39:06Z`

References
`url: https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_ds`
`↪s_v1-2.pdf`

Log (CVSS: 0.0)

NVT: MariaDB / Oracle MySQL Detection (MySQL Protocol)

Summary
MySQL protocol-based detection of MariaDB / Oracle MySQL.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected Oracle MySQL
Version:       5.0.51a-3ubuntu5
Location:      3306/tcp
CPE:           cpe:/a:oracle:mysql:5.0.51a
Concluded from version/product identification result:
5.0.51a-3ubuntu5
```

Solution:

Log Method
Details: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.100152
Version used: 2024-07-19T15:39:06Z

[return to 192.168.135.35]

2.1.52 Log 2121/tcp

Log (CVSS: 0.0)

NVT: SSL/TLS: FTP Missing Support For AUTH TLS

Summary
The remote FTP server does not support the 'AUTH TLS' command.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote FTP server does not support the 'AUTH TLS' command.

Solution:

Log Method
Details: SSL/TLS: FTP Missing Support For AUTH TLS
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: 2021-03-19T08:13:38Z

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
An FTP server is running on this port.
Here is its banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.135.35]

Solution:

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)

NVT: FTP Banner Detection

Summary
This script detects and reports a FTP Server Banner.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Remote FTP server banner:
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.135.35]
This is probably (a):
- ProFTPD
Server operating system information collected via "SYST" command:
215 UNIX Type: L8
```

Solution:

Log Method
Details: `FTP Banner Detection`
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: `2024-06-07T15:38:39Z`

Log (CVSS: 0.0)

NVT: ProFTPD Server Version Detection (Remote)

Summary
This script detects the installed version of ProFTP Server.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Detected ProFTPD
Version: 1.3.1
Location: 2121/tcp
CPE: cpe:/a:proftpd:proftpd:1.3.1
Concluded from version/product identification result:
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.135.35]

Solution:

Log Method
Details: ProFTPD Server Version Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.900815
Version used: 2021-09-01T14:04:04Z

[return to 192.168.135.35]

2.1.53 Log general/CPE-T

Log (CVSS: 0.0)

NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
192.168.135.35|cpe:/a:apache:http_server:2.2.8
192.168.135.35|cpe:/a:beasts:vsftpd:2.3.4
192.168.135.35|cpe:/a:ietf:secure_shell_protocol:2.0
192.168.135.35|cpe:/a:ietf:secure_sockets_layer:2.0
192.168.135.35|cpe:/a:ietf:secure_sockets_layer:3.0
192.168.135.35|cpe:/a:ietf:transport_layer_security:1.0
192.168.135.35|cpe:/a:isc:bind:9.4.2
192.168.135.35|cpe:/a:jquery:jquery:1.3.2
192.168.135.35|cpe:/a:mysql:mysql:5.0.51a

... continues on next page ...

... continued from previous page ...

```
192.168.135.35|cpe:/a:openbsd:openssh:4.7p1
192.168.135.35|cpe:/a:oracle:mysql:5.0.51a
192.168.135.35|cpe:/a:php:php:5.2.4
192.168.135.35|cpe:/a:phpmyadmin:phpmyadmin:3.1.1
192.168.135.35|cpe:/a:portmap:portmap
192.168.135.35|cpe:/a:postfix:postfix
192.168.135.35|cpe:/a:postgresql:postgresql:8.3.1
192.168.135.35|cpe:/a:proftpd:proftpd:1.3.1
192.168.135.35|cpe:/a:samba:samba:3.0.20
192.168.135.35|cpe:/a:twiki:twiki:01.Feb.2003
192.168.135.35|cpe:/a:unrealircd:unrealircd:3.2.8.1
192.168.135.35|cpe:/o:canonical:ubuntu_linux:8.04
```

Solution:

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: 2022-07-27T10:11:28Z

References
url: https://nvd.nist.gov/products/cpe

[return to 192.168.135.35]

2.1.54 Log 25/tcp

Log (CVSS: 0.0)

NVT: Postfix SMTP Server Detection (SMTP)

Summary
SMTP based detection of Postfix.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Postfix
Version:       unknown
Location:      25/tcp
CPE:           cpe:/a:postfix:postfix
Concluded from version/product identification result:
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: Postfix SMTP Server Detection (SMTP)
OID:1.3.6.1.4.1.25623.1.0.111086
Version used: 2024-01-12T05:05:56Z

References
url: https://www.postfix.org/

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Medium Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Non Weak Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:

... continues on next page ...

... continued from previous page ...

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
'Anonymous' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
```

... continues on next page ...

... continued from previous page ...

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
```

Solution:

Vulnerability Insight
Notes:
- As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-27T05:05:23Z

Log (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

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 (QoD): 98%

Vulnerability Detection Result

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher sui
↪tes 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 c
↪leartext communication.
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_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_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

... continues on next page ...

... continued from previous page ...

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
Version used: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

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`

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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
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
```

Log (CVSS: 0.0)

NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Protocol Version | Safe/Secure Renegotiation Support Status
--------------------------------------------------------------------------------
↪--------------------------------------------------------------------------------
↪-------------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.3          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)

NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
```

... continues on next page ...

... continued from previous page ...

00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652
↪E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complicati
↪on of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing
↪outside US,C=XX (Server certificate)

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
An SMTP server is running on this port
Here is its banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)

NVT: SMTP Server type and version

... continues on next page ...

... continued from previous page ...

Summary
This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Remote SMTP server banner:
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
The remote SMTP server is announcing the following available ESMTP commands (EHL
↪O response) via an unencrypted connection:
8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, V
↪RFY
```

Solution:

Log Method
Details: SMTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10263
Version used: 2024-09-25T05:06:11Z

Log (CVSS: 0.0)

NVT: SSL/TLS: SMTP 'STARTTLS' Command Detection

Summary
Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote SMTP server supports SSL/TLS with the 'STARTTLS' command.
The remote SMTP server is announcing the following available ESMTP commands (EHL
↪O response) before sending the 'STARTTLS' command:
8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, V
↪RFY
The remote SMTP server is announcing the following available ESMTP commands (EHL
↪O response) after sending the 'STARTTLS' command:
8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY
```

Solution:

Log Method
Details: SSL/TLS: SMTP 'STARTTLS' Command Detection

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103118
Version used: 2023-10-31T05:06:37Z

References
url: https://tools.ietf.org/html/rfc3207

Log (CVSS: 0.0)

NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
SSLv2
SSLv3
TLSv1.0

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: SSL/TLS: Version Detection
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)           | E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A
↪F1E32DEE436DE813CC
issued by                       | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00FAF93A4C7FB6B9CC
signature algorithm             | sha1WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
subject alternative names (SAN) | None
valid from                      | 2010-03-17 14:07:45 UTC
valid until                     | 2010-04-16 14:07:45 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate on this port is self-signed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The certificate of the remote service is self signed.

... continues on next page ...

... continued from previous page ...

```
Certificate details:
fingerprint (SHA-1)                | ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)              | E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A
↪F1E32DEE436DE813CC
issued by                          | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
public key algorithm               | RSA
public key size (bits)             | 1024
serial                             | 00FAF93A4C7FB6B9CC
signature algorithm                | sha1WithRSAEncryption
subject                            | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office
↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is
↪ no such thing outside US,C=XX
subject alternative names (SAN)    | None
valid from                         | 2010-03-17 14:07:45 UTC
valid until                        | 2010-04-16 14:07:45 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

[return to 192.168.135.35]