Scan Report

July 30, 2020

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 "Immediate scan of IP truerandom.bid". The scan started at and ended at . 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
161.35.97.88 truerandom.bid	3	12	0	0	0
Total: 1	3	12	0	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 15 results selected by the filtering described above. Before filtering there were 135 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
161.35.97.88 - truerandom.bid	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 161.35.97.88

Host scan start
Host scan end

Service (Port)	Threat Level
80/tcp	High
general/tcp	High
143/tcp	Medium
80/tcp	Medium
2525/tcp	Medium
995/tcp	Medium
993/tcp	Medium
110/tcp	Medium

2.1.1 High 80/tcp

High (CVSS: 7.5)
NVT: phpinfo() output Reporting

Summary
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 Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://truerandom.bid/phpinfo.php
```

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.

Vulnerability Detection Method
Details: `phpinfo() output Reporting`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2020-05-08T08:34:44+0000`

[return to 161.35.97.88]

2.1.2 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Source Edition (GSE)
- Greenbone Community Edition (GCE)

used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities

. . . continues on next page . . .

. . . continued from previous page . . .

- missing bugfixes
- incompatibilities within the feed.

Vulnerability Detection Result

```
Installed GVM Libraries (gvm-libs) version:        9.0.3
Latest available GVM Libraries (gvm-libs) version: 10.0.2
Reference URL(s) for the latest available version: https://community.greenbone.n
↪et/t/gvm-11-stable-initial-release-2019-10-14/3674 / https://community.greenbo
↪ne.net/t/gvm-10-old-stable-initial-release-2019-04-05/208
```

Solution

Solution type: VendorFix

Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.

If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.

Vulnerability Detection Method

Details: `Report outdated / end-of-life Scan Engine / Environment (local)`

OID:1.3.6.1.4.1.25623.1.0.108560

Version used: `2020-06-10T13:24:20+0000`

References

```
Other:
  URL:https://www.greenbone.net/en/install_use_gce/
   URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
↪03-07/211
   URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
↪04-05/208
   URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
↪4/3674
   URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
↪verride
   URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
↪verride
   URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
↪verride
```

High (CVSS: 10.0)
NVT: Important Announcement

Summary

ATTENTION:

. . . continues on next page . . .

... continued from previous page ...

Your vulnerability tests are out of maintenance and not updated since July 1st 2020. Your setup of Greenbone Source Edition will not report about any new threats in your scanned environment since this date!
REASON:
Your Greenbone setup is connected to a discontinued download protocol of the Greenbone Community Feed. The Greenbone Community Feed is still available via the preferred download protocol. The discontinuation announcement was posted on May 13th at the Greenbone Community Portal.
SOLUTION:
You can consider to upgrade your setup to a Greenbone enterprise product which also provides you the full scan coverage via Greenbone Security Feed (see PROFESSIONAL SOLUTION). Alternatively you can continue with the Greenbone Community Feed (see FREE COMMUNITY SOLUTION).
PROFESSIONAL SOLUTION (Upgrading to full coverage scanning)
We are happy that our technology already today helps you to reduce the attack surface of our corporate IT infrastructure. Our enterprise products close blind spots of the community feed and give access to Greenbone service desk.
Please contact
upgrade@greenbone.net
and provide the following details (use copy&paste). Please understand that we will not reply to you if you do not provide all the details.
- Company name: - Company homepage: - Your name: - Your position in the company: - The number of IP adresses you are scanning with Greenbone (ca.): - The number of scanner instances you are using to scan: - Are you using a master-sensor configuration: yes/no
Feel free to add any additional information you regard helpful to understand your setup.
Our team will recommend to you a suitable commercial option. We are happy to discuss larger setups in direct communication.
You can inform yourself about our standard products here:
https://www.greenbone.net/en/products-solutions/
FREE COMMUNITY SOLUTION: Continue scanning with community feed
The Greenbone Community Feed is still available and updated daily. You may have just missed the technical notes and announcement here:
https://community.greenbone.net/t/shutting-down-gcf-http-download/5339

Vulnerability Detection Result

```
ATTENTION:
Your vulnerability tests are out of maintenance and not updated since July 1st 2
↪020. Your setup of Greenbone Source Edition will not report about any new thre
↪ats in your scanned environment since this date!
REASON:
Your Greenbone setup is connected to a discontinued download protocol of the Gre
↪enbone Community Feed. The Greenbone Community Feed is still available via the
↪ preferred download protocol. The discontinuation announcement was posted on M
↪ay 13th at the Greenbone Community Portal.
SOLUTION:
You can consider to upgrade your setup to a Greenbone enterprise product which a
↪lso provides you the full scan coverage via Greenbone Security Feed (see PROFE
```

... continues on next page ...

. . . continued from previous page . . .

```
↪SSIONAL SOLUTION). Alternatively you can continue with the Greenbone Community
↪ Feed (see FREE COMMUNITY SOLUTION).
PROFESSIONAL SOLUTION (Upgrading to full coverage scanning)
We are happy that our technology already today helps you to reduce the attack su
↪rface of our corporate IT infrastructure. Our enterprise products close blind
↪spots of the community feed and give access to Greenbone service desk.
Please contact
upgrade@greenbone.net
and provide the following details (use copy&paste). Please understand that we wi
↪ll not reply to you if you do not provide all the details.
  - Company name:
  - Company homepage:
  - Your name:
  - Your position in the company:
  - The number of IP adresses you are scanning with Greenbone (ca.):
  - The number of scanner instances you are using to scan:
  - Are you using a master-sensor configuration: yes/no
Feel free to add any additional information you regard helpful to understand you
↪r setup.
Our team will recommend to you a suitable commercial option. We are happy to dis
↪cuss larger setups in direct communication.
You can inform yourself about our standard products here:
https://www.greenbone.net/en/products-solutions/
FREE COMMUNITY SOLUTION: Continue scanning with community feed
The Greenbone Community Feed is still available and updated daily. You may have
↪just missed the technical notes and announcement here:
https://community.greenbone.net/t/shutting-down-gcf-http-download/5339
```

Vulnerability Detection Method

Details: Important Announcement
OID:1.3.6.1.4.1.25623.1.0.999999
Version used: 2020-07-14T11:31:48+0000

References

Other:
  URL:https://community.greenbone.net/t/shutting-down-gcf-http-download/5339

[return to 161.35.97.88]

2.1.3 Medium 143/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary

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

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

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

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`

OID:1.3.6.1.4.1.25623.1.0.103440

Version used: `2020-03-31T06:57:15+0000`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
    URL:https://bettercrypto.org/
    URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

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).

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: `2020-03-31T06:57:15+0000`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 161.35.97.88]

2.1.4 Medium 80/tcp

Medium (CVSS: 5.0)

NVT: Source Control Management (SCM) Files Accessible

Summary

The script attempts to identify files of a SCM accessible at the webserver.

Vulnerability Detection Result

```
The following SCM files/folders were identified:
http://truerandom.bid/tools/windows-privesc-check/.git/logs/HEAD
http://truerandom.bid/tools/windows-privesc-check/.git/config
http://truerandom.bid/tools/windows-privesc-check/.git/info/exclude
http://truerandom.bid/tools/windows-privesc-check/.git/description
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://truerandom.bid/tools/windows-privesc-check/.git/HEAD
```

Impact
Based on the information provided in this files an attacker might be able to gather additional info about the structure of the system and its applications.

Solution
Solution type: Mitigation
Restrict access to the Admin Pages for authorized systems only.

Vulnerability Insight
Currently the script is checking for files of the following SCM:
- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

Vulnerability Detection Method
Check the response if SCM files are accessible.
Details: `Source Control Management (SCM) Files Accessible`
OID:1.3.6.1.4.1.25623.1.0.111084
Version used: `2020-05-06T06:57:16+0000`

References

```
Other:
  URL:http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-b
↪elong-to-us
    URL:https://github.com/anantshri/svn-extractor
    URL:https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d
    URL:https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/
    URL:http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/
```

[return to 161.35.97.88]

2.1.5 Medium 2525/tcp

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

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

Vulnerability Detection Result

```
'VRFY root' produces the following answer: 252 2.0.0 root
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: Workaround

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

Vulnerability Insight

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

Vulnerability Detection Method

Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `2020-03-23T13:51:29+0000`

References

```
Other:
  URL:http://cr.yp.to/smtp/vrfy.html
```

Medium (CVSS: 5.0)
NVT: SMTP Server on non standard port

Summary

This SMTP server is running on a non standard port.
This might be a backdoor set up by attackers to send spam or even control the system.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Solution type: Mitigation

Check and clean your configuration.

Vulnerability Detection Method

Details: `SMTP Server on non standard port`
OID:1.3.6.1.4.1.25623.1.0.18391
Version used: `2020-03-23T13:51:29+0000`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Solution

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

Vulnerability Insight

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

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2020-03-31T06:57:15+0000`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

[return to 161.35.97.88]

2.1.6 Medium 995/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary

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

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Solution

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

Vulnerability Insight

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

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2020-03-31T06:57:15+0000`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

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).

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: `2020-03-31T06:57:15+0000`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 161.35.97.88]

2.1.7 Medium 993/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

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

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`

OID:1.3.6.1.4.1.25623.1.0.103440

Version used: `2020-03-31T06:57:15+0000`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
    URL:https://bettercrypto.org/
    URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

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).

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: `2020-03-31T06:57:15+0000`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 161.35.97.88]

2.1.8 Medium 110/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).

- 1024 bit RSA authentication is considered to be insecure and therefore as weak.

- Any cipher considered to be secure for only the next 10 years is considered as medium

- Any other cipher is considered as strong

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`

OID:1.3.6.1.4.1.25623.1.0.103440

Version used: `2020-03-31T06:57:15+0000`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

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).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact

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

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2020-03-31T06:57:15+0000`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 161.35.97.88]

This file was automatically generated.