Scan Report

December 29, 2019

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 “kioptrix$_{s}can''.Thescanstartedatandendeda$

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.10.105	3	17	2	0	0
Total: 1	3	17	2	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 22 results selected by the filtering described above. Before filtering there were 153 results.

2 Results per Host

2.1 192.168.10.105

Host scan start
Host scan end

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

2.1.1 High 22/tcp

High (CVSS: 7.5)
NVT: Deprecated SSH-1 Protocol Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS

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

Vulnerability Detection Method

Details: `Deprecated SSH-1 Protocol Detection`

OID:1.3.6.1.4.1.25623.1.0.801993

Version used: `$Revision: 13586 $`

References

```
CVE: CVE-2001-0361, CVE-2001-0572, CVE-2001-1473
BID:2344
Other:
  URL:http://www.kb.cert.org/vuls/id/684820
   URL:http://xforce.iss.net/xforce/xfdb/6603
```

[return to 192.168.10.105]

2.1.2 High 443/tcp

High (CVSS: 7.5)
NVT: Webalizer Cross Site Scripting Vulnerability

Summary

Webalizer have a cross-site scripting vulnerability, that could allow malicious HTML tags to be injected in the reports generated by the Webalizer.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Upgrade to Version 2.01-09 and change the directory in 'OutputDir'.

Vulnerability Detection Method
Details: `Webalizer Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.10816
Version used: `2019-11-22T13:51:04+0000`

References
`CVE: CVE-2001-0835`
`BID:3473`

[return to 192.168.10.105]

2.1.3 High 80/tcp

High (CVSS: 7.5)
NVT: Webalizer Cross Site Scripting Vulnerability

Summary
Webalizer have a cross-site scripting vulnerability, that could allow malicious HTML tags to be injected in the reports generated by the Webalizer.

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

Solution
Solution type: VendorFix
Upgrade to Version 2.01-09 and change the directory in 'OutputDir'.

Vulnerability Detection Method
Details: `Webalizer Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.10816
Version used: `2019-11-22T13:51:04+0000`

References
`CVE: CVE-2001-0835`
`BID:3473`

[return to 192.168.10.105]

2.1.4 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
rijndael128-cbc
rijndael192-cbc
rijndael256-cbc
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
rijndael128-cbc
rijndael192-cbc
rijndael256-cbc
```

Solution
Solution type: Mitigation
Disable the weak encryption algorithms.

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: `SSH Weak Encryption Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `$Revision: 13581 $`

References

```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

[return to 192.168.10.105]

2.1.5 Medium 443/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.
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.

Vulnerability Detection Result

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

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

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

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
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2019-11-22T13:51:04+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683,
↪CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE
↪-2014-7883
BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995
Other:
  URL:http://www.kb.cert.org/vuls/id/288308
   URL:http://www.kb.cert.org/vuls/id/867593
   URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
   URL:https://www.owasp.org/index.php/Cross_Site_Tracing
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

Solution

Solution type: Mitigation

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

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

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `$Revision: 5232 $`

References

```
CVE: CVE-2016-2183, CVE-2016-6329
Other:
  URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://sweet32.info/
```

Medium (CVSS: 5.0)
NVT: Apache UserDir Sensitive Information Disclosure

Summary

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

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details: `Apache UserDir Sensitive Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10766
Version used: `2019-04-24T07:26:10+0000`

References

```
CVE: CVE-2001-1013
BID:3335
Other:
  URL:http://www.securiteam.com/unixfocus/5WP0C1F5FI.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

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

Vulnerability Detection Result

```
'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
```

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: `$Revision: 11872 $`

References

```
CVE: CVE-2015-4000
BID:74733
Other:
  URL:https://weakdh.org
   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-change
↪s
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

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

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 Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.
↪25623.1.0.802067) NVT.
```

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.

Solution
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ 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 containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used 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: `$Revision: 5547 $`

References

```
CVE: CVE-2016-0800, CVE-2014-3566
Other:
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://drownattack.com/
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary

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

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
- 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: `2019-07-05T09:29:25+0000`

References

```
CVE: CVE-2015-0204
BID:71936
Other:
  URL:https://freakattack.com
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
   URL:http://secpod.org/blog/?p=3818
   URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f
↪actoring-nsa.html
```

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 SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
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_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
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
```

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).

. . . continues on next page . . .

. . . continued from previous page . . .

- 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: `$Revision: 11135 $`

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: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `$Revision: 11402 $`

References

```
CVE: CVE-2014-3566
BID:70574
Other:
  URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   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-exploit
↪ing-ssl-30.html
```

Medium (CVSS: 4.3)
NVT: Apache Web Server ETag Header Information Disclosure Weakness

Summary

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Vulnerability Detection Result

```
Information that was gathered:
Inode: 34821
Size: 2890
```

Impact

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

Solution

Solution type: VendorFix

OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method

Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Details: `Apache Web Server ETag Header Information Disclosure Weakness`
OID:1.3.6.1.4.1.25623.1.0.103122
Version used: `2019-05-13T14:05:09+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2003-1418
BID:6939
Other:
  URL:https://www.securityfocus.com/bid/6939
   URL:http://httpd.apache.org/docs/mod/core.html#fileetag
   URL:http://www.openbsd.org/errata32.html
   URL:http://support.novell.com/docs/Tids/Solutions/10090670.html
```

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

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

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

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

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

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

Vulnerability Detection Method
Details: `Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: `$Revision: 11857 $`

References

```
CVE: CVE-2012-0053
BID:51706
Other:
  URL:http://secunia.com/advisories/47779
   URL:http://www.exploit-db.com/exploits/18442
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
    URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
    URL:http://httpd.apache.org/security/vulnerabilities_22.html
    URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
    URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

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.

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=#726F6F74406C6F63616C686F73742E6C6F63
↪616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrga
↪nization,L=SomeCity,ST=SomeState,C=--
Signature Algorithm:  md5WithRSAEncryption
```

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

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

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`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 11524 $`

References

```
Other:
  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).

Vulnerability Detection Result

```
Server Temporary Key Size: 512 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: `$Revision: 12865 $`

References

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

[return to 192.168.10.105]

2.1.6 Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.
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.

Vulnerability Detection Result

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

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

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

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
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2019-11-22T13:51:04+0000`

References

```
CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683,
↪CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE
↪-2014-7883
BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995
Other:
  URL:http://www.kb.cert.org/vuls/id/288308
   URL:http://www.kb.cert.org/vuls/id/867593
   URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
   URL:https://www.owasp.org/index.php/Cross_Site_Tracing
```

Medium (CVSS: 5.0)
NVT: Apache UserDir Sensitive Information Disclosure

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

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

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

Vulnerability Detection Method
Details: `Apache UserDir Sensitive Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10766
Version used: `2019-04-24T07:26:10+0000`

References
```
CVE: CVE-2001-1013
BID:3335
Other:
  URL:http://www.securiteam.com/unixfocus/5WP0C1F5FI.html
```

Medium (CVSS: 4.3)
NVT: Apache Web Server ETag Header Information Disclosure Weakness

Summary
A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Vulnerability Detection Result
```
Information that was gathered:
Inode: 34821
Size: 2890
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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

Solution

Solution type: VendorFix

OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method

Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Details: `Apache Web Server ETag Header Information Disclosure Weakness`

OID:1.3.6.1.4.1.25623.1.0.103122

Version used: `2019-05-13T14:05:09+0000`

References

```
CVE: CVE-2003-1418
BID:6939
Other:
  URL:https://www.securityfocus.com/bid/6939
    URL:http://httpd.apache.org/docs/mod/core.html#fileetag
    URL:http://www.openbsd.org/errata32.html
    URL:http://support.novell.com/docs/Tids/Solutions/10090670.html
```

Medium (CVSS: 4.3)

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

Summary

This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

Solution

Solution type: VendorFix

Upgrade to Apache HTTP Server version 2.2.22 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight

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

Vulnerability Detection Method

Details: `Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: `$Revision: 11857 $`

References

```
CVE: CVE-2012-0053
BID:51706
Other:
  URL:http://secunia.com/advisories/47779
   URL:http://www.exploit-db.com/exploits/18442
   URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 192.168.10.105]

2.1.7 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary

The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: `SSH Weak MAC Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `$Revision: 13581 $`

[return to 192.168.10.105]

2.1.8 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 87585
Packet 2: 87693
```

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

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

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

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP timestamps`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `$Revision: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 192.168.10.105]

This file was automatically generated.