# Consolidated

## 192.168.31.185

### 1

PHP 7.0.x < 7.0.9 Multiple Vulnerabilities (httpoxy)

PHP Vulnerability: CVE-2016-5385

PHP Vulnerability: CVE-2016-6289

PHP Vulnerability: CVE-2016-6290

PHP Vulnerability: CVE-2016-6291

PHP Vulnerability: CVE-2016-6292

PHP Vulnerability: CVE-2016-6294

PHP Vulnerability: CVE-2016-6295

PHP Vulnerability: CVE-2016-6296

PHP Vulnerability: CVE-2016-6297

PHP Man-in-the-Middle Attack Vulnerability July16 (Windows)

PHP Multiple Vulnerabilities-05 July16 (Windows)

# References

|  |  |  |  |
| --- | --- | --- | --- |
| CVE-2016-5385 |  |  |  |
| CVE-2016-5399 |  |  |  |
| CVE-2016-6128 |  |  |  |
| CVE-2016-6207 |  |  |  |
| CVE-2016-6288 |  |  |  |
| CVE-2016-6289 |  |  |  |
| CVE-2016-6290 |  |  |  |
| CVE-2016-6291 |  |  |  |
| CVE-2016-6292 |  |  |  |
| CVE-2016-6293 |  |  |  |
| CVE-2016-6294 |  |  |  |
| CVE-2016-6295 |  |  |  |
| CVE-2016-6296 |  |  |  |
| CVE-2016-6297 |  |  |  |

**BID**

|  |  |  |  |
| --- | --- | --- | --- |
| 91821 |  |  |  |

**CPE**

|  |  |  |  |
| --- | --- | --- | --- |
| cpe:/a:php:php |  |  |  |

**OSVDB**

|  |  |  |  |
| --- | --- | --- | --- |
| 141667 |  |  |  |

**CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| 797896 |  |  |  |

**EDB-ID**

|  |  |  |  |
| --- | --- | --- | --- |
| 40155 |  |  |  |

**REDHAT**

|  |  |  |  |
| --- | --- | --- | --- |
| RHSA-2016:1609 |  |  |  |

**APPLE**

|  |  |  |  |
| --- | --- | --- | --- |
| APPLE-SA-2016-09-20 |  |  |  |

**DFN-CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| DFN-CERT-2016-1367 |  |  |  |

### 2

OpenSSL 1.0.2 < 1.0.2f Multiple Vulnerabilities (Logjam)

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

OpenSSL SSLv2 doesn't block disabled ciphers (CVE-2015-3197)

OpenSSL DH small subgroups (CVE-2016-0701)

OpenSSL Multiple MitM Attack Vulnerabilities (Windows)

OpenSSL 'Diffie-Hellman small subgroups' MitM Attack Vulnerability (Windows)

# References

|  |  |  |  |
| --- | --- | --- | --- |
| CVE-2015-3197 |  |  |  |
| CVE-2015-4000 |  |  |  |
| CVE-2016-0701 |  |  |  |

**BID**

|  |  |  |  |
| --- | --- | --- | --- |
| 74733 |  |  |  |

**CPE**

|  |  |  |  |
| --- | --- | --- | --- |
| cpe:/a:openssl:openssl |  |  |  |

**OSVDB**

|  |  |  |  |
| --- | --- | --- | --- |
| 122331 |  |  |  |

**CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| 257823 |  |  |  |

**CERT-Bund**

|  |  |  |  |
| --- | --- | --- | --- |
| CB-K16/0168 |  |  |  |

**DFN-CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| DFN-CERT-2016-1174 |  |  |  |

### 3

OpenSSL 1.0.2 < 1.0.2g Multiple Vulnerabilities (DROWN)

OpenSSL Side channel attack on modular exponentiation (CVE-2016-0702)

OpenSSL Double-free in DSA code (CVE-2016-0705)

OpenSSL BN\_hex2bn/BN\_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797)

OpenSSL Memory leak in SRP database lookups (CVE-2016-0798)

OpenSSL Fix memory issues in BIO\_\*printf functions (CVE-2016-0799)

OpenSSL Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800)

OpenSSL Multiple Vulnerabilities -01 Mar16 (Windows)

OpenSSL SSLv2 DROWN Attack Vulnerability (Windows)

# References

|  |  |  |  |
| --- | --- | --- | --- |
| CVE-2016-0702 |  |  |  |
| CVE-2016-0705 |  |  |  |
| CVE-2016-0797 |  |  |  |
| CVE-2016-0798 |  |  |  |
| CVE-2016-0799 |  |  |  |
| CVE-2016-0800 |  |  |  |
| CVE-2016-2842 |  |  |  |

**BID**

|  |  |  |  |
| --- | --- | --- | --- |
| 83705 |  |  |  |

**CPE**

|  |  |  |  |
| --- | --- | --- | --- |
| cpe:/a:openssl:openssl |  |  |  |

**OSVDB**

|  |  |  |  |
| --- | --- | --- | --- |
| 134973 |  |  |  |

**CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| 583776 |  |  |  |

**DEBIAN**

|  |  |  |  |
| --- | --- | --- | --- |
| DSA-3500 |  |  |  |

**REDHAT**

|  |  |  |  |
| --- | --- | --- | --- |
| RHSA-2016:0722 |  |  |  |

**DFN-CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| DFN-CERT-2016-1401 |  |  |  |

### 4

HTTP TRACE / TRACK Methods Allowed

http TRACE XSS attack

HTTP TRACE Method Enabled

# References

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |  |  |  |

**BID**

|  |  |  |  |
| --- | --- | --- | --- |
| 9506 |  |  |  |

**OSVDB**

|  |  |  |  |
| --- | --- | --- | --- |
| 877 |  |  |  |

**CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| 288308 |  |  |  |

**CWE**

|  |  |  |  |
| --- | --- | --- | --- |
| 16 |  |  |  |

**CERT-Bund**

|  |  |  |  |
| --- | --- | --- | --- |
| CB-K14/0981 |  |  |  |

**DFN-CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| DFN-CERT-2014-1018 |  |  |  |

**APPLE**

|  |  |  |  |
| --- | --- | --- | --- |
| APPLE-SA-2009-11-09-1 |  |  |  |

**DISA\_SEVERITY**

|  |  |  |  |
| --- | --- | --- | --- |
| Category II |  |  |  |

**DISA\_VMSKEY**

|  |  |  |  |
| --- | --- | --- | --- |
| V0011706 |  |  |  |

**IAVM**

|  |  |  |  |
| --- | --- | --- | --- |
| 2005-T-0043 |  |  |  |

**OVAL**

|  |  |  |  |
| --- | --- | --- | --- |
| OVAL1445 |  |  |  |

**XF**

|  |  |  |  |
| --- | --- | --- | --- |
| 14959 |  |  |  |

### 5

OpenSSL 1.0.2 < 1.0.2h Multiple Vulnerabilities

OpenSSL EVP\_EncodeUpdate overflow (CVE-2016-2105)

OpenSSL EVP\_EncryptUpdate overflow (CVE-2016-2106)

OpenSSL Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)

OpenSSL ASN.1 BIO excessive memory allocation (CVE-2016-2109)

OpenSSL EBCDIC overread (CVE-2016-2176)

OpenSSL Multiple Vulnerabilities -01 May16 (Windows)

# References

|  |  |  |  |
| --- | --- | --- | --- |
| CVE-2016-2105 |  |  |  |
| CVE-2016-2106 |  |  |  |
| CVE-2016-2107 |  |  |  |
| CVE-2016-2109 |  |  |  |
| CVE-2016-2176 |  |  |  |

**BID**

|  |  |  |  |
| --- | --- | --- | --- |
| 87940 |  |  |  |

**CPE**

|  |  |  |  |
| --- | --- | --- | --- |
| cpe:/a:openssl:openssl |  |  |  |

**OSVDB**

|  |  |  |  |
| --- | --- | --- | --- |
| 137577 |  |  |  |

**EDB-ID**

|  |  |  |  |
| --- | --- | --- | --- |
| 39768 |  |  |  |

**IAVA**

|  |  |  |  |
| --- | --- | --- | --- |
| 2016-A-0113 |  |  |  |

**APPLE**

|  |  |  |  |
| --- | --- | --- | --- |
| APPLE-SA-2016-07-18-1 |  |  |  |

**DEBIAN**

|  |  |  |  |
| --- | --- | --- | --- |
| DSA-3566 |  |  |  |

**REDHAT**

|  |  |  |  |
| --- | --- | --- | --- |
| RHSA-2016:0722 |  |  |  |

**DFN-CERT**

|  |  |  |  |
| --- | --- | --- | --- |
| DFN-CERT-2016-1401 |  |  |  |

### 6

Apache HTTPD: HTTP\_PROXY environment variable "httpoxy" mitigation (CVE-2016-5387)

Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Windows)

# References

|  |  |  |
| --- | --- | --- |
| CVE-2016-5387 |  |  |

**BID**

|  |  |  |
| --- | --- | --- |
| 91816 |  |  |

**CERT**

|  |  |  |
| --- | --- | --- |
| 797896 |  |  |

**REDHAT**

|  |  |  |
| --- | --- | --- |
| RHSA-2016:1420 |  |  |

**DFN-CERT**

|  |  |  |
| --- | --- | --- |
| DFN-CERT-2016-1372 |  |  |

### 7

OpenSSL Pointer arithmetic undefined behaviour (CVE-2016-2177)

OpenSSL Constant time flag not preserved in DSA signing (CVE-2016-2178)

OpenSSL Multiple Vulnerabilities -19 Jun16 (Windows)

# References

|  |  |  |
| --- | --- | --- |
| CVE-2016-2177 |  |  |
| CVE-2016-2178 |  |  |

**BID**

|  |  |  |
| --- | --- | --- |
| 91319 |  |  |

**DFN-CERT**

|  |  |  |
| --- | --- | --- |
| DFN-CERT-2016-1136 |  |  |

### 8

TLS/SSL Server is enabling the POODLE attack

TLS/SSL Server Supports SSLv3

# References

|  |  |
| --- | --- |
| CVE-2014-3566 |  |

# 192.168.31.185

Hostname LAST-PC

Operating System Microsoft Windows 10 Home

## DCE Services Enumeration Severity: 0

49676/tcp | 135/tcp | 445/tcp | 2105/tcp | 2107/tcp | 2103/tcp | 49666/tcp | 49665/tcp | 49668/tcp | 49667/tcp | 49670/tcp | 49664/tcp

Summary

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

## PHP 7.0.x < 7.0.9 Multiple Vulnerabilities (httpoxy) Severity: 4 (Critical)

8080/tcp | 443/tcp

Summary

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP running on the remote web server is 7.0.x prior to 7.0.9. It is, therefore, affected by multiple vulnerabilities :  
  
 - A man-in-the-middle vulnerability exists, known as 'httpoxy', due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP\_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP\_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated. (CVE-2016-5385)  
  
 - An overflow condition exists in the php\_bz2iop\_read() function within file ext/bz2/bz2.c due to improper handling of error conditions. An unauthenticated, remote attacker can exploit this, via a crafted request, to execute arbitrary code. (CVE-2016-5399)  
  
 - A flaw exists in the GD Graphics Library (libgd), specifically in the gdImageScaleTwoPass() function within file gd\_interpolation.c, due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2016-6207)  
  
 - An integer overflow condition exists in the virtual\_file\_ex() function within file Zend/zend\_virtual\_cwd.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-6289)  
  
 - A use-after-free error exists within the file ext/session/session.c when handling 'var\_hash' destruction. An unauthenticated, remote attacker can exploit this to deference already freed memory, resulting in the execution of arbitrary code.  
 (CVE-2016-6290)  
  
 - An out-of-bounds read error exists in the exif\_process\_IFD\_in\_MAKERNOTE() function within file ext/exif/exif.c. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or disclose memory contents. (CVE-2016-6291)  
  
 - A NULL pointer dereference flaw exists in the exif\_process\_user\_comment() function within file ext/exif/exif.c. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.  
 (CVE-2016-6292)  
  
 - Multiple out-of-bounds read errors exist in the locale\_accept\_from\_http() function within file ext/intl/locale/locale\_methods.c. An unauthenticated, remote attacker can exploit these to cause a denial of service condition or disclose memory contents.  
 (CVE-2016-6293, CVE-2016-6294)  
  
 - A use-after-free error exists within file ext/snmp/snmp.c when handling garbage collection during deserialization of user-supplied input. An unauthenticated, remote attacker can exploit this to deference already freed memory, resulting in the execution of arbitrary code. (CVE-2016-6295)  
  
 - A heap-based buffer overflow condition exists in the simplestring\_addn() function within file simplestring.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-6296)  
  
 - An integer overflow condition exists in the php\_stream\_zip\_opener() function within file ext/zip/zip\_stream.c due to improper validation of user-supplied input when handling zip streams. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-6297)  
  
 - An out-of-bounds read error exists in the GD Graphics Library (libgd), specifically in the gdImageScaleBilinearPalette() function within file gd\_interpolation.c, when handling transparent color. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or disclose memory contents. (VulnDB 141674)  
  
 - A heap-based buffer overflow condition exists in the mdecrypt\_generic() function within file ext/mcrypt/mcrypt.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (VulnDB 141953)  
  
 - A flaw exists in the curl\_unescape() function within file ext/curl/interface.c when handling string lengths.  
 An unauthenticated, remote attacker can exploit this to cause heap corruption, resulting in a denial of service condition. (VulnDB 141955)  
  
 - A heap-based buffer overflow condition exists in the mcrypt\_generic() function within file ext/mcrypt/mcrypt.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (VulnDB 141956)  
  
 - A NULL write flaw exists in the GD Graphics Library (libgd) in the gdImageColorTransparent() function due to improper handling of negative transparent colors. A remote attacker can exploit this to disclose memory contents. (VulnDB 142104)

Solution

Upgrade to PHP version 7.0.9 or later.

CVSS (Base Score)

10.0 CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS (Temporal Score)

7.8 CVSS2#E:POC/RL:OF/RC:ND

References

**BID**

91821

92051

92073

92074

92078

92094

92095

92097

92099

**CPE**

cpe:/a:php:php

**CVE**

CVE-2016-5385

CVE-2016-5399

CVE-2016-6207

CVE-2016-6289

CVE-2016-6290

CVE-2016-6291

CVE-2016-6292

CVE-2016-6293

CVE-2016-6294

CVE-2016-6295

CVE-2016-6296

CVE-2016-6297

**OSVDB**

141667

141674

141675

141942

141943

141944

141945

141946

141953

141954

141955

141956

141957

141958

142018

142104

**CERT**

797896

**EDB-ID**

40155

References Links

http://php.net/ChangeLog-7.php#7.0.9

https://httpoxy.org

## PHP Version Severity: 0

8080/tcp | 443/tcp

Summary

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

References

**CPE**

cpe:/a:php:php

## OpenSSL 1.0.2 < 1.0.2f Multiple Vulnerabilities (Logjam) Severity: 2 (Medium)

8080/tcp | 443/tcp

Summary

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSL 1.0.2 prior to 1.0.2f. It is, therefore, affected by the following vulnerabilities :  
  
 - A cipher algorithm downgrade vulnerability exists due to a flaw that is triggered when handling cipher negotiation. A remote attacker can exploit this to negotiate SSLv2 ciphers and complete SSLv2 handshakes even if all SSLv2 ciphers have been disabled on the server. Note that this vulnerability only exists if the SSL\_OP\_NO\_SSLv2 option has not been disabled.  
 (CVE-2015-3197)  
  
 - A man-in-the-middle vulnerability, known as Logjam, exists due to a flaw in the SSL/TLS protocol. A remote attacker can exploit this flaw to downgrade connections using ephemeral Diffie-Hellman key exchange to 512-bit export-grade cryptography. (CVE-2015-4000)  
  
 - An information disclosure vulnerability exists due to a flaw in the DH\_check\_pub\_key() function that is triggered when generating DH parameters based on unsafe primes. A remote attacker can exploit this, via multiple handshakes, to disclose the private DH exponent.  
 (CVE-2016-0701)

Solution

Upgrade to OpenSSL version 1.0.2f or later.

CVSS (Base Score)

4.3 CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS (Temporal Score)

3.7 CVSS2#E:F/RL:TF/RC:ND

References

**BID**

74733

**CPE**

cpe:/a:openssl:openssl

**CVE**

CVE-2015-3197

CVE-2015-4000

CVE-2016-0701

**OSVDB**

122331

133714

133715

**CERT**

257823

References Links

https://www.openssl.org/news/secadv/20160128.txt

https://weakdh.org/

## OpenSSL 1.0.2 < 1.0.2g Multiple Vulnerabilities (DROWN) Severity: 3 (High)

8080/tcp | 443/tcp

Summary

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSL 1.0.2 prior to 1.0.2g. It is, therefore, affected by the following vulnerabilities :  
  
 - A key disclosure vulnerability exists due to improper handling of cache-bank conflicts on the Intel Sandy-bridge microarchitecture. An attacker can exploit this to gain access to RSA key information.  
 (CVE-2016-0702)  
  
 - A double-free error exists due to improper validation of user-supplied input when parsing malformed DSA private keys. A remote attacker can exploit this to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2016-0705)  
  
 - A NULL pointer dereference flaw exists in the BN\_hex2bn() and BN\_dec2bn() functions. A remote attacker can exploit this to trigger a heap corruption, resulting in the execution of arbitrary code. (CVE-2016-0797)  
  
 - A denial of service vulnerability exists due to improper handling of invalid usernames. A remote attacker can exploit this, via a specially crafted username, to leak 300 bytes of memory per connection, exhausting available memory resources. (CVE-2016-0798)  
  
 - Multiple memory corruption issues exist that allow a remote attacker to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-0799)  
  
 - A flaw exists that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption).  
 This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key. (CVE-2016-0800)

Solution

Upgrade to OpenSSL version 1.0.2g or later.

CVSS (Base Score)

9.3 CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS (Temporal Score)

6.9 CVSS2#E:U/RL:OF/RC:C

References

**BID**

83705

83733

83754

83755

83763

**CPE**

cpe:/a:openssl:openssl

**CVE**

CVE-2016-0702

CVE-2016-0705

CVE-2016-0797

CVE-2016-0798

CVE-2016-0799

CVE-2016-0800

**OSVDB**

134973

135095

135096

135121

135149

135150

135151

**CERT**

583776

References Links

https://www.openssl.org/news/secadv/20160301.txt

https://www.openssl.org/news/cl102.txt

https://drownattack.com/

https://www.drownattack.com/drown-attack-paper.pdf

## HyperText Transfer Protocol (HTTP) Redirect Information Severity: 0

8080/tcp | 443/tcp

Summary

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.  
  
This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

## Web Server Office File Inventory Severity: 0

8080/tcp | 443/tcp

Summary

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

References

**CPE**

cpe:/a:microsoft:office

## HTTP TRACE / TRACK Methods Allowed Severity: 2 (Medium)

8080/tcp | 443/tcp

Summary

Debugging functions are enabled on the remote web server.

Description

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

Solution

Disable these methods. Refer to the plugin output for more information.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS (Temporal Score)

4.3 CVSS2#E:H/RL:OF/RC:C

References

**BID**

9506

9561

11604

33374

37995

**CVE**

CVE-2003-1567

CVE-2004-2320

CVE-2010-0386

**OSVDB**

877

3726

5648

11408

50485

**CERT**

288308

867593

**CWE**

16

References Links

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\_XST\_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

## Missing or Permissive X-Frame-Options HTTP Response Header Severity: 0

8080/tcp | 443/tcp

Summary

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.  
  
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

Solution

Set a properly configured X-Frame-Options header for all requested resources.

References Links

http://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

## Web Application Sitemap Severity: 0

8080/tcp | 443/tcp

Summary

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

References Links

http://www.nessus.org/u?5496c8d9

## External URLs Severity: 0

8080/tcp | 443/tcp

Summary

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

## Web mirroring Severity: 0

8080/tcp | 443/tcp

Summary

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.  
  
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

## Web Server Directory Enumeration Severity: 0

8080/tcp | 443/tcp

Summary

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

References

**OWASP**

OWASP-CM-006

References Links

http://projects.webappsec.org/Predictable-Resource-Location

## Link-Local Multicast Name Resolution (LLMNR) Detection Severity: 0

5355/udp

Summary

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

References Links

http://www.nessus.org/u?85beb421

http://technet.microsoft.com/en-us/library/bb878128.aspx

## mDNS Detection (Local Network) Severity: 0

5353/udp

Summary

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.  
  
This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

## Service Detection Severity: 0

3306/tcp | 80/tcp | 443/tcp | 8080/tcp | 443/tcp

Summary

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

## SMB Signing Disabled Severity: 2 (Medium)

445/tcp

Summary

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS (Temporal Score)

3.7 CVSS2#E:U/RL:OF/RC:C

References

**CPE**

cpe:/o:microsoft:windows  
cpe:/a:samba:samba

References Links

https://support.microsoft.com/en-us/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

## Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry Severity: 0

445/tcp

Summary

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.  
  
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

## Nessus TCP scanner Severity: 0

445/tcp | 135/tcp | 139/tcp | 443/tcp | 8080/tcp | 2107/tcp | 2105/tcp | 3306/tcp | 2103/tcp | 1801/tcp | 80/tcp

Summary

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.  
  
Once a TCP connection is open, it grabs any available banner for the service identification plugins.  
  
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

## Microsoft Windows SMB Log In Possible Severity: 0

445/tcp

Summary

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :  
  
- NULL session  
- Guest account  
- Supplied credentials

References Links

http://support.microsoft.com/kb/143474

http://support.microsoft.com/kb/246261

## Microsoft Windows SMB NativeLanManager Remote System Information Disclosure Severity: 0

445/tcp

Summary

It is possible to obtain information about the remote operating system.

Description

It is possible to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. This script requires SMB1 enabled on the host.

## Microsoft Windows SMB Service Detection Severity: 0

445/tcp | 139/tcp

Summary

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

## CGI Generic Tests HTTP Errors Severity: 0

443/tcp | 8080/tcp

Summary

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :  
  
 - Network -> Network Receive Timeout (check\_read\_timeout)  
  
 - Options -> Number of hosts in parallel (max\_hosts)  
  
 - Options -> Number of checks in parallel (max\_checks)

## CGI Generic Tests Load Estimation (all tests) Severity: 0

443/tcp | 8080/tcp

Summary

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.  
  
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.  
  
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

## OpenSSL 1.0.2 < 1.0.2h Multiple Vulnerabilities Severity: 2 (Medium)

443/tcp | 8080/tcp

Summary

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSL 1.0.2 prior to 1.0.2h. It is, therefore, affected by the following vulnerabilities :  
  
 - A heap buffer overflow condition exists in the EVP\_EncodeUpdate() function within file crypto/evp/encode.c that is triggered when handling a large amount of input data. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2016-2105)  
  
 - A heap buffer overflow condition exists in the EVP\_EncryptUpdate() function within file crypto/evp/evp\_enc.c that is triggered when handling a large amount of input data after a previous call occurs to the same function with a partial block. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2016-2106)  
  
 - Flaws exist in the aesni\_cbc\_hmac\_sha1\_cipher() function in file crypto/evp/e\_aes\_cbc\_hmac\_sha1.c and the aesni\_cbc\_hmac\_sha256\_cipher() function in file crypto/evp/e\_aes\_cbc\_hmac\_sha256.c that are triggered when the connection uses an AES-CBC cipher and AES-NI is supported by the server. A man-in-the-middle attacker can exploit these to conduct a padding oracle attack, resulting in the ability to decrypt the network traffic.  
 (CVE-2016-2107)  
  
 - Multiple unspecified flaws exist in the d2i BIO functions when reading ASN.1 data from a BIO due to invalid encoding causing a large allocation of memory.  
 An unauthenticated, remote attacker can exploit these to cause a denial of service condition through resource exhaustion. (CVE-2016-2109)  
  
 - An out-of-bounds read error exists in the X509\_NAME\_oneline() function within file crypto/x509/x509\_obj.c when handling very long ASN1 strings. An unauthenticated, remote attacker can exploit this to disclose the contents of stack memory.  
 (CVE-2016-2176)

Solution

Upgrade to OpenSSL version 1.0.2h or later.

CVSS (Base Score)

5.8 CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSS (Temporal Score)

4.5 CVSS2#E:POC/RL:OF/RC:C

References

**BID**

87940

89744

89746

89757

89760

**CPE**

cpe:/a:openssl:openssl

**CVE**

CVE-2016-2105

CVE-2016-2106

CVE-2016-2107

CVE-2016-2109

CVE-2016-2176

**OSVDB**

137577

137896

137897

137898

137899

**EDB-ID**

39768

**IAVA**

2016-A-0113

References Links

https://www.openssl.org/news/secadv/20160503.txt

https://www.openssl.org/news/cl102.txt

## OpenSSL Version Detection Severity: 0

443/tcp | 8080/tcp

Summary

The version of OpenSSL can be identified.

Description

The version of OpenSSL could be extracted from the web server's banner. Note that in many cases, security patches are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

References

**CPE**

cpe:/a:openssl:openssl

References Links

http://www.openssl.org/

## Browsable Web Directories Severity: 2 (Medium)

443/tcp | 8080/tcp

Summary

Some directories on the remote web server are browsable.

Description

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

References Links

http://www.nessus.org/u?0a35179e

## HSTS Missing From HTTPS Server Severity: 0

443/tcp

Summary

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution

Configure the remote web server to use HSTS.

References Links

https://tools.ietf.org/html/rfc6797

## Apache mod\_info /server-info Information Disclosure Severity: 2 (Medium)

443/tcp | 8080/tcp

Summary

The remote web server discloses information about its configuration.

Description

It is possible to obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

Solution

If required, update Apache's configuration file(s) to either disable mod\_info or ensure that access is limited to valid users / hosts.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CPE**

cpe:/a:apache:http\_server

**OSVDB**

562

References Links

http://httpd.apache.org/docs/mod/mod\_info.html

## Apache mod\_status /server-status Information Disclosure Severity: 2 (Medium)

443/tcp | 8080/tcp

Summary

The remote web server discloses information about its status.

Description

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Solution

If required, update Apache's configuration file(s) to either disable mod\_status or ensure that access is limited to valid users / hosts.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CPE**

cpe:/a:apache:http\_server

**OSVDB**

561

## HTTP Methods Allowed (per directory) Severity: 0

443/tcp | 80/tcp | 8080/tcp

Summary

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.  
  
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.  
  
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

## PHP expose\_php Information Disclosure Severity: 2 (Medium)

443/tcp | 8080/tcp

Summary

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.  
  
Other such Easter eggs likely exist, but Nessus has not checked for them.

Solution

In the PHP configuration file, php.ini, set the value for 'expose\_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CPE**

cpe:/a:php:php

**OSVDB**

12184

References Links

http://www.0php.com/php\_easter\_egg.php

http://seclists.org/webappsec/2004/q4/324

## HTTP Server Type and Version Severity: 0

443/tcp | 80/tcp | 8080/tcp

Summary

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

## SSL Certificate with Wrong Hostname Severity: 2 (Medium)

443/tcp

Summary

The SSL certificate for this service is for a different host.

Description

The commonName (CN) of the SSL certificate presented on this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

CVSS (Base Score)

5.0 CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

## Missing or Permissive Content-Security-Policy HTTP Response Header Severity: 0

443/tcp | 8080/tcp

Summary

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.  
  
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

References Links

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

## SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) Severity: 1 (Low)

443/tcp

Summary

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

CVSS (Base Score)

2.6 CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

References

**BID**

74733

**CPE**

cpe:/a:openssl:openssl

**CVE**

CVE-2015-4000

**OSVDB**

122331

References Links

http://weakdh.org/

## SSL Cipher Block Chaining Cipher Suites Supported Severity: 0

443/tcp

Summary

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

References Links

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

## SSL Perfect Forward Secrecy Cipher Suites Supported Severity: 0

443/tcp

Summary

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

References Links

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman\_key\_exchange

http://en.wikipedia.org/wiki/Perfect\_forward\_secrecy

## SSL Cipher Suites Supported Severity: 0

443/tcp

Summary

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

References Links

https://www.openssl.org/docs/manmaster/apps/ciphers.html

http://www.nessus.org/u?7d537016

## SSL Certificate Cannot Be Trusted Severity: 2 (Medium)

443/tcp

Summary

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.  
  
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.  
  
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.  
  
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  
  
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper certificate for this service.

CVSS (Base Score)

6.4 CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

## SSL Certificate Signed Using Weak Hashing Algorithm Severity: 2 (Medium)

443/tcp

Summary

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.  
  
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.  
  
Note that certificates in the chain that are contained in the Nessus CA database have been ignored.

Solution

Contact the Certificate Authority to have the certificate reissued.

CVSS (Base Score)

4.0 CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N

CVSS (Temporal Score)

3.5 CVSS2#E:ND/RL:OF/RC:C

References

**BID**

11849

33065

**CPE**

cpe:/a:ietf:md5  
cpe:/a:ietf:x.509\_certificate

**CVE**

CVE-2004-2761

**OSVDB**

45106

45108

45127

**CERT**

836068

**CWE**

310

References Links

http://tools.ietf.org/html/rfc3279

http://www.phreedom.org/research/rogue-ca/

http://technet.microsoft.com/en-us/security/advisory/961509

## SSL Self-Signed Certificate Severity: 2 (Medium)

443/tcp

Summary

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.  
  
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

CVSS (Base Score)

6.4 CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

## OpenSSL Detection Severity: 0

443/tcp

Summary

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.  
  
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

References

**CPE**

cpe:/a:openssl:openssl

References Links

http://www.openssl.org

## SSL Certificate Information Severity: 0

443/tcp

Summary

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

## SSL Certificate commonName Mismatch Severity: 0

443/tcp

Summary

The SSL certificate commonName does not match the host name.

Description

This service presents an SSL certificate for which the 'commonName' (CN) does not match the host name on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS host name that matches the common name in the certificate.

## TLS ALPN Supported Protocol Enumeration Severity: 0

443/tcp

Summary

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

References Links

https://tools.ietf.org/html/rfc7301

## SSL / TLS Versions Supported Severity: 0

443/tcp

Summary

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

## Nessus SYN scanner Severity: 0

443/tcp | 135/tcp | 139/tcp | 445/tcp | 80/tcp | 2103/tcp | 8080/tcp | 1801/tcp | 3306/tcp | 2107/tcp | 2105/tcp

Summary

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.  
  
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

## NetBIOS Multiple IP Address Enumeration Severity: 0

137/udp

Summary

The remote host is configured with multiple IP addresses.

Description

By sending a special NetBIOS query, Nessus was able to detect the use of multiple IP addresses on the remote host. This indicates the host may be running virtualization software, a VPN client, or has multiple network interfaces.

## Windows NetBIOS / SMB Remote Host Information Disclosure Severity: 0

137/udp

Summary

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.  
  
Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

## HyperText Transfer Protocol (HTTP) Information Severity: 0

80/tcp | 8080/tcp | 443/tcp

Summary

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...  
  
This test is informational only and does not denote any security problem.

## Traceroute Information Severity: 0

Summary

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

## Nessus Scan Information Severity: 0

Summary

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :  
  
 - The version of the plugin set.  
 - The type of scanner (Nessus or Nessus Home).  
 - The version of the Nessus Engine.  
 - The port scanner(s) used.  
 - The port range scanned.  
 - Whether credentialed or third-party patch management checks are possible.  
 - The date of the scan.  
 - The duration of the scan.  
 - The number of hosts scanned in parallel.  
 - The number of checks done in parallel.

## Patch Report Severity: 0

Summary

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

## Device Type Severity: 0

Summary

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

## Common Platform Enumeration (CPE) Severity: 0

Summary

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.  
  
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

References Links

http://cpe.mitre.org/

https://nvd.nist.gov/cpe.cfm

## OS Identification Severity: 0

Summary

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

## Ethernet Card Manufacturer Detection Severity: 0

Summary

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

References Links

http://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

## TCP/IP Timestamps Supported Severity: 0

Summary

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

References Links

http://www.ietf.org/rfc/rfc1323.txt

# 192.168.31.185

Hostname Last-Pc

Operating System Windows  
 FreeBSD 6.2-RELEASE  
 Windows 7 Professional Edition  
 Windows Server 2008  
 Windows 7.5  
 Windows Server 2008 R2  
 Windows Vista

## Apache HTTPD: Padding Oracle in Apache mod\_session\_crypto (CVE-2016-0736) Severity: 4

80/tcp | 443/tcp

Description

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod\_session\_crypto. Review your web server configuration for validation. Prior to Apache HTTP release 2.4.25, mod\_sessioncrypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Solution

Apache HTTPD >= 2.4 and < 2.4.25  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

4.4 AV:L/AC:M/Au:N/C:P/I:P/A:P

References

**CVE**

CVE-2016-0736

References Links

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

3, fail

Tag

Apache, Apache HTTP Server, Web

## Apache HTTPD: mod\_http2: denial of service by thread starvation (CVE-2016-1546) Severity: 4

80/tcp | 443/tcp

Description

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod\_http2. Review your web server configuration for validation. By manipulating the flow control windows on streams, a client was able to block server threads for long times, causing starvation of worker threads. Connections could still be opened, but no streams where processed for these. This issue affected HTTP/2 support in 2.4.17 and 2.4.18.

Solution

Apache HTTPD >= 2.4 and < 2.4.20  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.20.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:N/A:P

References

**BID**

92331

**CVE**

CVE-2016-1546

References Links

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

2, pass

Tag

Apache, Apache HTTP Server, Denial of Service, Web

## Apache HTTPD: DoS vulnerability in mod\_auth\_digest (CVE-2016-2161) Severity: 4

80/tcp | 443/tcp

Description

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod\_auth\_digest. Review your web server configuration for validation. Malicious input to mod\_auth\_digest will cause the server to crash, and each instance continues to crash even for subsequently valid requests.

Solution

Apache HTTPD >= 2.4 and < 2.4.25  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

4.4 AV:L/AC:M/Au:N/C:P/I:P/A:P

References

**CVE**

CVE-2016-2161

References Links

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

3, fail

Tag

Apache, Apache HTTP Server, Denial of Service, Web

## Apache HTTPD: TLS/SSL X.509 client certificate auth bypass with HTTP/2 (CVE-2016-4979) Severity: 5

80/tcp | 443/tcp

Description

For configurations enabling support for HTTP/2, SSL client certificate validation was not enforced if configured, allowing clients unauthorized access to protected resources over HTTP/2. This issue affected releases 2.4.18 and 2.4.20 only.

Solution

Apache HTTPD >= 2.4 and < 2.4.23  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.23.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N

References

**BID**

91566

**CVE**

CVE-2016-4979

**REDHAT**

RHSA-2016:1420

References Links

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

3, fail

Tag

Apache, Apache HTTP Server, Web

## Apache HTTPD: HTTP\_PROXY environment variable "httpoxy" mitigation (CVE-2016-5387) Severity: 5

80/tcp | 443/tcp

Description

HTTP\_PROXY is a well-defined environment variable in a CGI process, which collided with a number of libraries which failed to avoid colliding with this CGI namespace. A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP\_PROXY" variable from a "Proxy:" header, which has never been registered by IANA. This workaround and patch are documented in the ASF Advisory at https://www.apache.org/security/asf-httpoxy-response.txt

Solution

Apache HTTPD >= 2.2 and < 2.2.32  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.2.32.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.  
Apache HTTPD >= 2.4 and < 2.4.25  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

5.1 AV:N/AC:H/Au:N/C:P/I:P/A:P

References

**BID**

91816

**CERT**

797896

**CVE**

CVE-2016-5387

**REDHAT**

RHSA-2016:1420

RHSA-2016:1421

RHSA-2016:1422

RHSA-2016:1624

RHSA-2016:1625

RHSA-2016:1635

RHSA-2016:1636

RHSA-2016:1648

RHSA-2016:1649

RHSA-2016:1650

RHSA-2016:1851

References Links

http://httpd.apache.org/security/vulnerabilities\_22.html

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

3, fail

Tag

Apache, Apache HTTP Server, Web

## Apache HTTPD: HTTP/2 CONTINUATION denial of service (CVE-2016-8740) Severity: 5

80/tcp | 443/tcp

Description

The HTTP/2 protocol implementation (mod\_http2) had an incomplete handling of the LimitRequestFields directive. This allowed an attacker to inject unlimited request headers into the server, leading to eventual memory exhaustion.

Solution

Apache HTTPD >= 2.4 and < 2.4.25  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

94650

**CVE**

CVE-2016-8740

References Links

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

2, pass

Tag

Apache, Apache HTTP Server, Denial of Service, Web

## Apache HTTPD: Apache HTTP Request Parsing Whitespace Defects (CVE-2016-8743) Severity: 4

80/tcp | 443/tcp

Description

Apache HTTP Server, prior to release 2.4.25, accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member "the\_request", while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. RFC7230 Section 3.5 calls out some of these whitespace exceptions, and section 3.2.3 eliminated and clarified the role of implied whitespace in the grammer of this specification. Section 3.1.1 requires exactly one single SP between the method and request-target, and between the request-target and HTTP-version, followed immediately by a CRLF sequence. None of these fields permit any (unencoded) CTL character whatsoever. Section 3.2.4 explicitly disallowed any whitespace from the request header field prior to the ':' character, while Section 3.2 disallows all CTL characters in the request header line other than the HTAB character as whitespace. These defects represent a security concern when httpd is participating in any chain of proxies or interacting with back-end application servers, either through mod\_proxy or using conventional CGI mechanisms. In each case where one agent accepts such CTL characters and does not treat them as whitespace, there is the possiblity in a proxy chain of generating two responses from a server behind the uncautious proxy agent. In a sequence of two requests, this results in request A to the first proxy being interpreted as requests A + A' by the backend server, and if requests A and B were submitted to the first proxy in a keepalive connection, the proxy may interpret response A' as the response to request B, polluting the cache or potentially serving the A' content to a different downstream user-agent. These defects are addressed with the release of Apache HTTP Server 2.4.25 and coordinated by a new directive; HttpProtocolOptions Strict which is the default behavior of 2.4.25 and later. By toggling from 'Strict' behavior to 'Unsafe' behavior, some of the restrictions may be relaxed to allow some invalid HTTP/1.1 clients to communicate with the server, but this will reintroduce the possibility of the problems described in this assessment. Note that relaxing the behavior to 'Unsafe' will still not permit raw CTLs other than HTAB (where permitted), but will allow other RFC requirements to not be enforced, such as exactly two SP characters in the request line.

Solution

Apache HTTPD >= 2.4 and < 2.4.25  
Download and apply the upgrade from:  
http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz  
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

CVSS (Base Score)

4.4 AV:L/AC:M/Au:N/C:P/I:P/A:P

References

**CVE**

CVE-2016-8743

References Links

http://httpd.apache.org/security/vulnerabilities\_22.html

http://httpd.apache.org/security/vulnerabilities\_24.html

Pci

3, fail

Tag

Apache, Apache HTTP Server, Web

## X.509 Certificate Subject CN Does Not Match the Entity Name Severity: 7

443/tcp | 465/tcp | 995/tcp

Description

The subject common name (CN) field in the X.509 certificate does not match  
the name of the entity presenting the certificate. Before issuing a certificate, a Certification Authority (CA) must check the  
identity of the entity requesting the certificate, as specified in the CA's  
Certification Practice Statement (CPS). Thus, standard certificate validation  
procedures require the subject CN field of a certificate to match the actual  
name of the entity presenting the certificate. For example, in a certificate  
presented by "https://www.example.com/", the CN should be "www.example.com". In order to detect and prevent active eavesdropping attacks, the validity of  
a certificate must be verified, or else an attacker could then launch a  
man-in-the-middle attack and gain full control of the data stream. Of  
particular importance is the validity of the subject's CN, that should match  
the name of the entity (hostname). A CN mismatch most often occurs due to a configuration error, though it can  
also indicate that a man-in-the-middle attack is being conducted.

Solution

The subject's common name (CN) field in the X.509 certificate should be fixed  
to reflect the name of the entity presenting the certificate (e.g., the  
hostname). This is done by generating a new certificate usually signed by a  
Certification Authority (CA) trusted by both the client and server.

CVSS (Base Score)

7.1 AV:N/AC:H/Au:N/C:C/I:C/A:N

Pci

5, fail

Tag

HTTP, Web

## Database Open Access Severity: 5

3306/tcp

Description

The database allows any remote system the ability to connect to it. It is   
 recommended to limit direct access to trusted systems because databases may   
 contain sensitive data, and new vulnerabilities and exploits are discovered   
 routinely for them. For this reason, it is a violation of PCI DSS section   
 1.3.6 to have databases listening on ports accessible from the Internet,   
 even when protected with secure authentication mechanisms.

Solution

Configure the database server to only allow access to trusted systems.  
 For example, the PCI DSS standard requires you to place the database in an   
 internal network zone, segregated from the DMZ

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

References Links

https://www.pcisecuritystandards.org/documents/PCI\_DSS\_v3-1.pdf

Pci

3, fail

Tag

Database, Network

## TCP timestamp response Severity: 1

Description

The remote host responded with a TCP timestamp. The TCP timestamp response  
 can be used to approximate the remote host's uptime, potentially aiding in  
 further attacks. Additionally, some operating systems can be fingerprinted  
 based on the behavior of their TCP timestamps.

Solution

Cisco  
Run the following command to disable TCP timestamps:  
no ip tcp timestamp  
FreeBSD  
Set the value of net.inet.tcp.rfc1323 to 0 by running the   
 following command:  
sysctl -w net.inet.tcp.rfc1323=0  
Additionally, put the following value in the default sysctl  
 configuration file, generally sysctl.conf:  
net.inet.tcp.rfc1323=0  
Linux  
Set the value of net.ipv4.tcp\_timestamps to 0 by running the   
 following command:  
sysctl -w net.ipv4.tcp\_timestamps=0  
Additionally, put the following value in the default sysctl  
 configuration file, generally sysctl.conf:  
net.ipv4.tcp\_timestamps=0  
OpenBSD  
Set the value of net.inet.tcp.rfc1323 to 0 by running the   
 following command:  
sysctl -w net.inet.tcp.rfc1323=0  
Additionally, put the following value in the default sysctl  
 configuration file, generally sysctl.conf:  
net.inet.tcp.rfc1323=0  
Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition  
Set the Tcp1323Opts value in the following key to 1:  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  
Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Storage Server 2012, Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta  
TCP timestamps cannot be reliably disabled on this OS. If TCP timestamps present enough of a risk, put a firewall capable of blocking TCP timestamp packets in front of the affected assets.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

References Links

http://uptime.netcraft.com

http://www.forensicswiki.org/wiki/TCP\_timestamps

http://www.ietf.org/rfc/rfc1323.txt

Pci

1, pass

Tag

Network

## Apache Server mod\_info is Publicly Accessible Severity: 5

80/tcp | 443/tcp

Description

The web server publicly offers a report on its configuration to anyone who requests it,  
 revealing sensitive details that give a potential attacker important information about how  
 to attack the web server.

Solution

The configuration file for apache (httpd.conf), reads:  
<Location /server-info>  
 SetHandler server-info  
 </Location>  
To remove the feature from Apache, rewrite this to:  
# comment everything out  
 #<Location /server-info>  
 # SetHandler server-info  
 #</Location>  
To keep the feature, adding access control, rewrite it to:  
# add access control  
 <Location/server-info>  
 SetHandler server-info  
  
 Order deny,allow  
 Deny from all  
 Allow from 127.0.0.1  
 </Location>  
Once these changes have been made, the Apache server needs to be restarted.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

Pci

3, fail

Tag

Apache, Apache HTTP Server, HTTP, Web

## Apache Server mod\_status is Publicly Accessible Severity: 4

80/tcp | 443/tcp

Description

The web server publicly offers a report on its current state to anyone  
 who requests it, revealing details that could give a potential attacker  
 information about how to attack the web server.

Solution

The configuration file for apache (httpd.conf), reads:  
<Location /server-status>  
 SetHandler server-status  
 </Location>  
To remove the feature from Apache, rewrite this to:  
# comment everything out  
 #<Location /server-status>  
 # SetHandler server-status  
 #</Location>  
To keep the feature, adding access control, rewrite this to:  
# add access control  
 <Location/server-status>  
 SetHandler server-status   
 Order deny,allow  
 Deny from all  
 Allow from 127.0.0.1  
 </Location>  
Once these changes have been made, the Apache server needs to be restarted.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

Pci

3, fail

Tag

Apache, Apache HTTP Server, HTTP, Web

## Default CGI Script printenv is Executable Severity: 4

80/tcp | 443/tcp

Description

The web server makes a test script available that reveals details  
 of the web server's configuration to anyone who can connect to the machine.

Solution

Look for the file "printenv" in your Apache installation tree, usually  
 in a directory called "cgi-bin", either move this file or delete it.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

Pci

3, fail

Tag

Apache, Apache HTTP Server, HTTP, Web

## OpenSSL SSLv2 doesn't block disabled ciphers (CVE-2015-3197) Severity: 4

80/tcp | 443/tcp

Description

ssl/s2\_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get\_client\_master\_key and get\_client\_hello functions.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1r.tar.gz  
Upgrade to version 1.0.1r of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1r.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2f.tar.gz  
Upgrade to version 1.0.2f of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2f.tar.gz

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**BID**

82237

91787

**CERT**

257823

**CVE**

CVE-2015-3197

References Links

https://www.openssl.org/news/secadv/20160128.txt

Pci

3, fail

Tag

HTTP, OpenSSL, Web

## OpenSSL DH small subgroups (CVE-2016-0701) Severity: 3

80/tcp | 443/tcp

Description

The DH\_check\_pub\_key function in crypto/dh/dh\_check.c in OpenSSL 1.0.2 before 1.0.2f does not ensure that prime numbers are appropriate for Diffie-Hellman (DH) key exchange, which makes it easier for remote attackers to discover a private DH exponent by making multiple handshakes with a peer that chose an inappropriate number, as demonstrated by a number in an X9.42 file.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2f.tar.gz  
Upgrade to version 1.0.2f of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2f.tar.gz

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N

References

**BID**

82233

91787

**CERT**

257823

**CVE**

CVE-2016-0701

References Links

https://www.openssl.org/news/secadv/20160128.txt

Pci

2, pass

Tag

HTTP, OpenSSL, Web

## OpenSSL Side channel attack on modular exponentiation (CVE-2016-0702) Severity: 2

80/tcp | 443/tcp

Description

The MOD\_EXP\_CTIME\_COPY\_FROM\_PREBUF function in crypto/bn/bn\_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a "CacheBleed" attack.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Upgrade to version 1.0.1s of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz  
Upgrade to version 1.0.2g of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz

CVSS (Base Score)

1.9 AV:L/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2016-0702

**DEBIAN**

DSA-3500

References Links

https://www.openssl.org/news/secadv/20160301.txt

Pci

1, pass

Tag

HTTP, OpenSSL, Web

## OpenSSL Double-free in DSA code (CVE-2016-0705) Severity: 10

80/tcp | 443/tcp

Description

Double free vulnerability in the dsa\_priv\_decode function in crypto/dsa/dsa\_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Upgrade to version 1.0.1s of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz  
Upgrade to version 1.0.2g of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz

CVSS (Base Score)

10.0 AV:N/AC:L/Au:N/C:C/I:C/A:C

References

**BID**

83754

91787

**CVE**

CVE-2016-0705

**DEBIAN**

DSA-3500

References Links

https://www.openssl.org/news/secadv/20160301.txt

Pci

5, fail

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL BN\_hex2bn/BN\_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797) Severity: 5

80/tcp | 443/tcp

Description

Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN\_dec2bn or (2) BN\_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn\_print.c.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Upgrade to version 1.0.1s of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz  
Upgrade to version 1.0.2g of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

83763

91787

**CVE**

CVE-2016-0797

**DEBIAN**

DSA-3500

References Links

https://www.openssl.org/news/secadv/20160301.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Memory leak in SRP database lookups (CVE-2016-0798) Severity: 8

80/tcp | 443/tcp

Description

Memory leak in the SRP\_VBASE\_get\_by\_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s\_server.c and crypto/srp/srp\_vfy.c.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Upgrade to version 1.0.1s of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz  
Upgrade to version 1.0.2g of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz

CVSS (Base Score)

7.8 AV:N/AC:L/Au:N/C:N/I:N/A:C

References

**BID**

83705

91787

**CVE**

CVE-2016-0798

**DEBIAN**

DSA-3500

References Links

https://www.openssl.org/news/secadv/20160301.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Fix memory issues in BIO\_\*printf functions (CVE-2016-0799) Severity: 10

80/tcp | 443/tcp

Description

The fmtstr function in crypto/bio/b\_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Upgrade to version 1.0.1s of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz  
Upgrade to version 1.0.2g of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz

CVSS (Base Score)

10.0 AV:N/AC:L/Au:N/C:C/I:C/A:C

References

**BID**

83755

91787

**CVE**

CVE-2016-0799

**DEBIAN**

DSA-3500

**REDHAT**

RHSA-2016:0722

RHSA-2016:0996

References Links

https://www.openssl.org/news/secadv/20160301.txt

Pci

5, fail

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800) Severity: 4

80/tcp | 443/tcp

Description

The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Upgrade to version 1.0.1s of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1s.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz  
Upgrade to version 1.0.2g of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2g.tar.gz

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**BID**

83733

91787

**CERT**

583776

**CVE**

CVE-2016-0800

**REDHAT**

RHSA-2016:1519

References Links

https://www.openssl.org/news/secadv/20160301.txt

Pci

3, fail

Tag

HTTP, OpenSSL, Web

## OpenSSL EVP\_EncodeUpdate overflow (CVE-2016-2105) Severity: 5

80/tcp | 443/tcp

Description

Integer overflow in the EVP\_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Upgrade to version 1.0.1t of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz  
Upgrade to version 1.0.2h of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**APPLE**

APPLE-SA-2016-07-18-1

**BID**

89757

91787

**CVE**

CVE-2016-2105

**DEBIAN**

DSA-3566

**REDHAT**

RHSA-2016:0722

RHSA-2016:0996

RHSA-2016:1648

RHSA-2016:1649

RHSA-2016:1650

References Links

https://www.openssl.org/news/secadv/20160503.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL EVP\_EncryptUpdate overflow (CVE-2016-2106) Severity: 5

80/tcp | 443/tcp

Description

Integer overflow in the EVP\_EncryptUpdate function in crypto/evp/evp\_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Upgrade to version 1.0.1t of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz  
Upgrade to version 1.0.2h of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**APPLE**

APPLE-SA-2016-07-18-1

**BID**

89744

91787

**CVE**

CVE-2016-2106

**DEBIAN**

DSA-3566

**REDHAT**

RHSA-2016:0722

RHSA-2016:0996

RHSA-2016:1648

RHSA-2016:1649

RHSA-2016:1650

References Links

https://www.openssl.org/news/secadv/20160503.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Padding oracle in AES-NI CBC MAC check (CVE-2016-2107) Severity: 3

80/tcp | 443/tcp

Description

The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session, NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Upgrade to version 1.0.1t of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz  
Upgrade to version 1.0.2h of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N

References

**APPLE**

APPLE-SA-2016-07-18-1

**BID**

89760

91787

**CVE**

CVE-2016-2107

**DEBIAN**

DSA-3566

**REDHAT**

RHSA-2016:0722

RHSA-2016:0996

References Links

**exploitdb  
 OpenSSL - Padding Oracle in AES-NI CBC MAC Check**

http://www.exploit-db.com/exploits/39768

https://www.openssl.org/news/secadv/20160503.txt

Pci

2, pass

Tag

HTTP, OpenSSL, Web

## OpenSSL ASN.1 BIO excessive memory allocation (CVE-2016-2109) Severity: 8

80/tcp | 443/tcp

Description

The asn1\_d2i\_read\_bio function in crypto/asn1/a\_d2i\_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Upgrade to version 1.0.1t of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz  
Upgrade to version 1.0.2h of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz

CVSS (Base Score)

7.8 AV:N/AC:L/Au:N/C:N/I:N/A:C

References

**APPLE**

APPLE-SA-2016-07-18-1

**BID**

87940

91787

**CVE**

CVE-2016-2109

**DEBIAN**

DSA-3566

**REDHAT**

RHSA-2016:0722

RHSA-2016:0996

References Links

https://www.openssl.org/news/secadv/20160503.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL EBCDIC overread (CVE-2016-2176) Severity: 6

80/tcp | 443/tcp

Description

The X509\_NAME\_oneline function in crypto/x509/x509\_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Upgrade to version 1.0.1t of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1t.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz  
Upgrade to version 1.0.2h of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2h.tar.gz

CVSS (Base Score)

6.4 AV:N/AC:L/Au:N/C:P/I:N/A:P

References

**APPLE**

APPLE-SA-2016-07-18-1

**BID**

89746

91787

**CVE**

CVE-2016-2176

References Links

https://www.openssl.org/news/secadv/20160503.txt

Pci

4, fail

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Pointer arithmetic undefined behaviour (CVE-2016-2177) Severity: 4

80/tcp | 443/tcp

Description

OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3\_srvr.c, ssl\_sess.c, and t1\_lib.c.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:N/A:P

References

**BID**

91319

**CVE**

CVE-2016-2177

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Constant time flag not preserved in DSA signing (CVE-2016-2178) Severity: 2

80/tcp | 443/tcp

Description

The dsa\_sign\_setup function in crypto/dsa/dsa\_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

2.1 AV:L/AC:L/Au:N/C:P/I:N/A:N

References

**BID**

91081

**CVE**

CVE-2016-2178

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

HTTP, OpenSSL, Web

## OpenSSL DTLS buffered message DoS (CVE-2016-2179) Severity: 5

80/tcp | 443/tcp

Description

The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1\_lib.c, statem\_dtls.c, statem\_lib.c, and statem\_srvr.c.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92987

**CVE**

CVE-2016-2179

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL OOB read in TS\_OBJ\_print\_bio() (CVE-2016-2180) Severity: 5

80/tcp | 443/tcp

Description

The TS\_OBJ\_print\_bio function in crypto/ts/ts\_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92117

**CVE**

CVE-2016-2180

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL DTLS replay protection DoS (CVE-2016-2181) Severity: 5

80/tcp | 443/tcp

Description

The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec\_layer\_d1.c and ssl3\_record.c.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92982

**CVE**

CVE-2016-2181

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL OOB write in BN\_bn2dec() (CVE-2016-2182) Severity: 8

80/tcp | 443/tcp

Description

The BN\_bn2dec function in crypto/bn/bn\_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92557

**CVE**

CVE-2016-2182

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

5, fail

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Malformed SHA512 ticket DoS (CVE-2016-6302) Severity: 5

80/tcp | 443/tcp

Description

The tls\_decrypt\_ticket function in ssl/t1\_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92628

**CVE**

CVE-2016-6302

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL OOB write in MDC2\_Update() (CVE-2016-6303) Severity: 8

80/tcp | 443/tcp

Description

Integer overflow in the MDC2\_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92984

**CVE**

CVE-2016-6303

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

5, fail

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL OCSP Status Request extension unbounded memory growth (CVE-2016-6304) Severity: 8

80/tcp | 443/tcp

Description

Multiple memory leaks in t1\_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.1.0a.tar.gz  
Upgrade to version 1.1.0a of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.1.0a.tar.gz

CVSS (Base Score)

7.8 AV:N/AC:L/Au:N/C:N/I:N/A:C

References

**BID**

93150

**CVE**

CVE-2016-6304

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## OpenSSL Certificate message OOB reads (CVE-2016-6306) Severity: 4

80/tcp | 443/tcp

Description

The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3\_clnt.c and s3\_srvr.c.

Solution

Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Upgrade to version 1.0.1u of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.1u.tar.gz  
Download and apply the upgrade from:  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz  
Upgrade to version 1.0.2i of  
OpenSSL  
http://www.openssl.org  
OpenSSL's website  
http://ftp.openssl.org/source/openssl-1.0.2i.tar.gz

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:N/A:P

References

**BID**

93153

**CVE**

CVE-2016-6306

References Links

https://www.openssl.org/news/secadv/20160922.txt

Pci

2, pass

Tag

Denial of Service, HTTP, OpenSSL, Web

## HTTP TRACE Method Enabled Severity: 6

80/tcp | 443/tcp

Description

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Solution

Apache HTTPD  
Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a  
 configuration directive called TraceEnable. To deny TRACE requests,  
 add the following line to the server configuration:  
TraceEnable off  
For older versions of the Apache webserver, use the mod\_rewrite module to  
 deny the TRACE requests:  
RewriteEngine On  
RewriteCond %{REQUEST\_METHOD} ^TRACE  
RewriteRule .\* - [F]  
IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS  
For Microsoft Internet Information Services (IIS), you may  
 use the URLScan tool, freely available at  
http://www.microsoft.com/technet/security/tools/urlscan.mspx  
http://www.microsoft.com/technet/security/tools/urlscan.mspx  
Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet  
For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the  
 following configuration to the top of the default object in the  
 'obj.conf' file:  
<Client method="TRACE">  
 AuthTrans fn="set-variable"  
 remove-headers="transfer-encoding"  
 set-headers="content-length: -1"  
 error="501"  
</Client>  
You must then restart the server for the changes to take effect.  
For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the  
 instructions provided the 'Relief/Workaround' section of  
 Sun's official advisory:  
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603  
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603  
Lotus Domino  
Follow  
IBM's instructions  
http://www-1.ibm.com/support/docview.wss?&uid=swg21201202  
HTTPDisableMethods=TRACE  
After saving NOTES.INI, restart the Notes web server by issuing the console  
 command "tell http restart".

CVSS (Base Score)

5.8 AV:N/AC:M/Au:N/C:P/I:P/A:N

References

**APPLE**

APPLE-SA-2009-11-09-1

**BID**

15222

19915

24456

36956

9506

**CERT**

867593

**CVE**

CVE-2004-2320

CVE-2004-2763

CVE-2005-3398

CVE-2006-4683

CVE-2007-3008

CVE-2008-7253

CVE-2009-2823

CVE-2010-0386

**DISA\_SEVERITY**

Category II

**DISA\_VMSKEY**

V0011706

**IAVM**

2005-T-0043

**OSVDB**

35511

3726

**OVAL**

OVAL1445

**XF**

14959

34854

References Links

**metasploit  
 HTTP Options Detection**

http://www.metasploit.com/modules/auxiliary/scanner/http/options

http://www.apacheweek.com/issues/03-01-24#news

http://www.kb.cert.org/vuls/id/867593

Pci

3, fail

Tag

HTTP, Web, XSS, IAVM

## PHP Vulnerability: CVE-2016-5385 Severity: 5

80/tcp | 443/tcp

Description

PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP\_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP\_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.1 AV:N/AC:H/Au:N/C:P/I:P/A:P

References

**BID**

91821

**CERT**

797896

**CVE**

CVE-2016-5385

**REDHAT**

RHSA-2016:1609

RHSA-2016:1610

RHSA-2016:1611

RHSA-2016:1612

RHSA-2016:1613

Pci

3, fail

Tag

HTTP, PHP, Web

## PHP Vulnerability: CVE-2016-6289 Severity: 7

80/tcp | 443/tcp

Description

Integer overflow in the virtual\_file\_ex function in TSRM/tsrm\_virtual\_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

6.8 AV:N/AC:M/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92074

**CVE**

CVE-2016-6289

References Links

https://bugs.php.net/72513

Pci

4, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-6290 Severity: 8

80/tcp | 443/tcp

Description

ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92097

**CVE**

CVE-2016-6290

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-6291 Severity: 8

80/tcp | 443/tcp

Description

The exif\_process\_IFD\_in\_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92073

**CVE**

CVE-2016-6291

References Links

https://bugs.php.net/72603

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-6292 Severity: 4

80/tcp | 443/tcp

Description

The exif\_process\_user\_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:N/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92078

**CVE**

CVE-2016-6292

Pci

2, pass

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-6294 Severity: 8

80/tcp | 443/tcp

Description

The locale\_accept\_from\_http function in ext/intl/locale/locale\_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc\_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92115

**CVE**

CVE-2016-6294

References Links

https://bugs.php.net/72533

Pci

5, fail

Tag

Denial of Service, HTTP, PHP, Web

## PHP Vulnerability: CVE-2016-6295 Severity: 8

80/tcp | 443/tcp

Description

ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92094

**CVE**

CVE-2016-6295

References Links

https://bugs.php.net/72479

Pci

5, fail

Tag

Denial of Service, HTTP, PHP, SNMP

## PHP Vulnerability: CVE-2016-6296 Severity: 8

80/tcp | 443/tcp

Description

Integer signedness error in the simplestring\_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc\_encode\_request function.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92095

**CVE**

CVE-2016-6296

Pci

5, fail

Tag

Denial of Service, HTTP, PHP, RPC

## PHP Vulnerability: CVE-2016-6297 Severity: 7

80/tcp | 443/tcp

Description

Integer overflow in the php\_stream\_zip\_opener function in ext/zip/zip\_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

6.8 AV:N/AC:M/Au:N/C:P/I:P/A:P

References

**APPLE**

APPLE-SA-2016-09-20

**BID**

92099

**CVE**

CVE-2016-6297

Pci

4, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7124 Severity: 8

80/tcp | 443/tcp

Description

ext/standard/var\_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) \_\_destruct call or (2) magic method call.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92756

**CVE**

CVE-2016-7124

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7125 Severity: 5

80/tcp | 443/tcp

Description

ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N

References

**BID**

92552

**CVE**

CVE-2016-7125

Pci

3, fail

Tag

HTTP, PHP

## PHP Vulnerability: CVE-2016-7126 Severity: 8

80/tcp | 443/tcp

Description

The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select\_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92755

**CVE**

CVE-2016-7126

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7127 Severity: 8

80/tcp | 443/tcp

Description

The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92757

**CVE**

CVE-2016-7127

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7128 Severity: 5

80/tcp | 443/tcp

Description

The exif\_process\_IFD\_in\_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**BID**

92564

**CVE**

CVE-2016-7128

Pci

3, fail

Tag

HTTP, PHP

## PHP Vulnerability: CVE-2016-7129 Severity: 8

80/tcp | 443/tcp

Description

The php\_wddx\_process\_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx\_deserialize call that mishandles a dateTime element in a wddxPacket XML document.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92758

**CVE**

CVE-2016-7129

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7130 Severity: 5

80/tcp | 443/tcp

Description

The php\_wddx\_pop\_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx\_deserialize call that mishandles a binary element in a wddxPacket XML document.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92764

**CVE**

CVE-2016-7130

Pci

2, pass

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7131 Severity: 5

80/tcp | 443/tcp

Description

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx\_deserialize call, as demonstrated by a tag that lacks a < (less than) character.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92768

**CVE**

CVE-2016-7131

Pci

2, pass

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7132 Severity: 5

80/tcp | 443/tcp

Description

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx\_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

92767

**CVE**

CVE-2016-7132

Pci

2, pass

Tag

Denial of Service, HTTP, Mail, PHP

## PHP Vulnerability: CVE-2016-7133 Severity: 7

80/tcp | 443/tcp

Description

Zend/zend\_alloc.c in PHP 7.x before 7.0.10, when open\_basedir is enabled, mishandles huge realloc operations, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a long pathname.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

6.8 AV:N/AC:M/Au:N/C:P/I:P/A:P

References

**BID**

92765

**CVE**

CVE-2016-7133

Pci

4, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7134 Severity: 8

80/tcp | 443/tcp

Description

ext/curl/interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer overflow, which allows remote attackers to cause a denial of service (allocation error and heap-based buffer overflow) or possibly have unspecified other impact via a long string that is mishandled in a curl\_escape call.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

92766

**CVE**

CVE-2016-7134

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7412 Severity: 7

80/tcp | 443/tcp

Description

ext/mysqlnd/mysqlnd\_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED\_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

6.8 AV:N/AC:M/Au:N/C:P/I:P/A:P

References

**BID**

93005

**CVE**

CVE-2016-7412

Pci

4, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7413 Severity: 8

80/tcp | 443/tcp

Description

Use-after-free vulnerability in the wddx\_stack\_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx\_deserialize call.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

93006

**CVE**

CVE-2016-7413

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7414 Severity: 8

80/tcp | 443/tcp

Description

The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed\_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

93004

**CVE**

CVE-2016-7414

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7416 Severity: 5

80/tcp | 443/tcp

Description

ext/intl/msgformat/msgformat\_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

93008

**CVE**

CVE-2016-7416

Pci

2, pass

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7417 Severity: 8

80/tcp | 443/tcp

Description

ext/spl/spl\_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**BID**

93007

**CVE**

CVE-2016-7417

Pci

5, fail

Tag

Denial of Service, HTTP, PHP

## PHP Vulnerability: CVE-2016-7418 Severity: 5

80/tcp | 443/tcp

Description

The php\_wddx\_push\_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx\_deserialize call.

Solution

Download and apply the upgrade from:  
http://www.php.net/releases/  
Download and apply the upgrade from:  
http://www.php.net/releases/

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

References

**BID**

93011

**CVE**

CVE-2016-7418

Pci

2, pass

Tag

Denial of Service, HTTP, PHP

## TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566) Severity: 4

465/tcp | 995/tcp

Description

Recent cryptanalysis results exploit biases in the RC4 keystream to recover repeatedly encrypted  
 plaintexts. As a result, RC4 can no longer be seen as providing a sufficient level of security  
 for SSL/TLS sessions. It has many single-byte biases, which makes it easier for remote attackers to conduct  
 plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use  
 the same plaintext.

Solution

Configure the server to disable support for RC4 ciphers.  
For Microsoft IIS web servers, see Microsoft Knowledgebase article  
245030  
http://support.microsoft.com/kb/245030/  
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.  
Refer to your server vendor documentation to apply the recommended cipher configuration:  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2013-2566

References Links

http://www.isg.rhul.ac.uk/tls/

https://tools.ietf.org/html/rfc7465

http://www.nist.gov/manuscript-publication-search.cfm?pub\_id=915295

https://wiki.mozilla.org/Security/Server\_Side\_TLS

https://www.owasp.org/index.php/Transport\_Layer\_Protection\_Cheat\_Sheet#Rule\_-\_Only\_Support\_Strong\_Cryptographic\_Ciphers

http://support.microsoft.com/kb/245030/

Pci

3, fail

Tag

Network

## TLS/SSL Server Supports 3DES Cipher Suite Severity: 1

443/tcp | 465/tcp | 995/tcp

Description

Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the  
 3DES (Triple Data Encryption Standard) algorithm.  
 Since 3DES only provides an effective security of 112 bits, it is considered close to end of life by some agencies. Consequently, the 3DES algorithm is not included in the specifications for TLS version 1.3.  
 ECRYPT II (from 2012) recommends for generic application independent long-term protection at least 128 bits security. The same recommendation has also been reported by BSI Germany (from 2015) and ANSSI France (from 2014), 128 bit is the recommended symmetric size and should be mandatory after 2020. While NIST (from 2012) still considers 3DES being appropriate to use until the end of 2030.

Solution

Configure the server to disable support for 3DES suite.  
For Microsoft IIS web servers, see Microsoft Knowledgebase article  
245030  
http://support.microsoft.com/kb/245030/  
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.  
Refer to your server vendor documentation to apply the recommended cipher configuration:  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

CVSS (Base Score)

0.0 AV:N/AC:H/Au:N/C:N/I:N/A:N

References Links

http://www.nist.gov/manuscript-publication-search.cfm?pub\_id=915295

http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

https://wiki.mozilla.org/Security/Server\_Side\_TLS

https://www.owasp.org/index.php/Transport\_Layer\_Protection\_Cheat\_Sheet#Rule\_-\_Only\_Support\_Strong\_Cryptographic\_Ciphers

http://support.microsoft.com/kb/245030/

Pci

1, pass

Tag

Network

## TLS/SSL Server is enabling the BEAST attack Severity: 4

443/tcp | 465/tcp | 995/tcp

Description

The SSL protocol, as used in certain configurations of Microsoft Windows and browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (and other products negotiating SSL connections) encrypts data by using CBC mode with chained initialization vectors. This potentially allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. By supporting the affected protocols and ciphers, the server is enabling the clients in to being exploited.

Solution

There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected  
 protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD),  
 e.g. AES-GCM, AES-CCM in TLS 1.2.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2011-3389

References Links

http://vnhacker.blogspot.co.uk/2011/09/beast.html

Pci

3, fail

Tag

Network

## TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) Severity: 5

443/tcp | 465/tcp | 995/tcp

Description

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC  
 mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption  
 cipher are affected. The security of a block cipher is often reduced to the key size k: the best attack should  
 be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an  
 important security parameter, defining the amount of data that can be encrypted under the same key. This is  
 particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to  
 the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than 2  
 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such  
 as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday  
 bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks  
 occurs it is possible to use the collision to extract the plain text data.

Solution

Configure the server to disable support for 3DES suite.  
For Microsoft IIS web servers, see Microsoft Knowledgebase article  
245030  
http://support.microsoft.com/kb/245030/  
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.  
Refer to your server vendor documentation to apply the recommended cipher configuration:  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2016-2183

References Links

https://sweet32.info/

https://www.openssl.org/blog/blog/2016/08/24/sweet32

https://access.redhat.com/articles/2548661

Pci

3, fail

Tag

Network, Rapid7 Critical

## TLS/SSL Server Supports DES and IDEA Cipher Suites Severity: 6

443/tcp

Description

Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on  
 the DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) algorithms. DES and IDEA  
 algorithms are no longer recommended for general use in TLS, and have been removed from TLS version 1.2.

Solution

Configure the server to disable support for DES and IDEA cipher suites.  
For Microsoft IIS web servers, see Microsoft Knowledgebase article  
245030  
http://support.microsoft.com/kb/245030/  
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.  
Refer to your server vendor documentation to apply the recommended cipher configuration:  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

CVSS (Base Score)

5.8 AV:N/AC:M/Au:N/C:P/I:P/A:N

References Links

http://www.nist.gov/manuscript-publication-search.cfm?pub\_id=915295

https://wiki.mozilla.org/Security/Server\_Side\_TLS

https://www.owasp.org/index.php/Transport\_Layer\_Protection\_Cheat\_Sheet#Rule\_-\_Only\_Support\_Strong\_Cryptographic\_Ciphers

http://support.microsoft.com/kb/245030/

https://tools.ietf.org/html/rfc5469

Pci

3, fail

Tag

Network

## Self-signed TLS/SSL certificate Severity: 4

443/tcp | 465/tcp | 995/tcp

Description

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be  
 trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use  
 self-signed certificates to eavesdrop on TLS/SSL connections.

Solution

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server.  
 The exact instructions for obtaining a new certificate depend on your organization's requirements.  
 Generally, you will need to generate a certificate request and save the request as a file. This  
 file is then sent to a Certificate Authority (CA) for processing. Your organization may have its  
 own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted  
 external Certificate Authority, such as  
Thawte  
http://www.thawte.com  
Verisign  
http://www.verisign.com

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:P/A:N

Pci

3, fail

Tag

Network

## TLS/SSL Server Supports The Use of Static Key Ciphers Severity: 3

443/tcp | 465/tcp | 995/tcp

Description

The server is configured to support ciphers known as static key ciphers. These ciphers don't support  
 "Forward Secrecy". In the new specification for HTTP/2, these ciphers have been blacklisted.

Solution

Configure the server to disable support for static key cipher suites.  
For Microsoft IIS web servers, see Microsoft Knowledgebase article  
245030  
http://support.microsoft.com/kb/245030/  
The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.  
Refer to your server vendor documentation to apply the recommended cipher configuration:  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N

References Links

http://www.nist.gov/manuscript-publication-search.cfm?pub\_id=915295

https://wiki.mozilla.org/Security/Server\_Side\_TLS

https://www.owasp.org/index.php/Transport\_Layer\_Protection\_Cheat\_Sheet#Rule\_-\_Only\_Support\_Strong\_Cryptographic\_Ciphers

http://support.microsoft.com/kb/245030/

https://tools.ietf.org/html/rfc7540/

Pci

2, pass

Tag

Network

## TLS/SSL Server is enabling the POODLE attack Severity: 4

465/tcp | 995/tcp

Description

All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks. The SSL 3.0 vulnerability stems from the way blocks of data are encrypted under a specific type of encryption algorithm within the SSL protocol. The POODLE attack takes advantage of the protocol version negotiation feature built into SSL to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session. The Payment Card Industry (PCI) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard also requires a minimum of TLS v1.1 and recommends TLS v1.2.

Solution

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2014-3566

References Links

**metasploit  
 HTTP SSL/TLS Version Detection (POODLE scanner)**

http://www.metasploit.com/modules/auxiliary/scanner/http/ssl\_version

https://www.pcisecuritystandards.org/documents/Migrating\_from\_SSL\_Early\_TLS\_Information%20Supplement\_v1.pdf

https://www.us-cert.gov/ncas/alerts/TA14-290A

Pci

3, fail

Tag

Network, Web

## TLS/SSL Server Supports SSLv3 Severity: 4

465/tcp | 995/tcp

Description

The SSLv3 protocol and supported ciphers all suffer from serious vulnerabilities making this protocol unsafe to use. The Payment Card Industry (PCI) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard also requires a minimum of TLS v1.1 and recommends TLS v1.2.

Solution

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2014-3566

References Links

**metasploit  
 HTTP SSL/TLS Version Detection (POODLE scanner)**

http://www.metasploit.com/modules/auxiliary/scanner/http/ssl\_version

https://www.pcisecuritystandards.org/documents/Migrating\_from\_SSL\_Early\_TLS\_Information%20Supplement\_v1.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Pci

3, fail

Tag

Network

## Diffie-Hellman group smaller than 2048 bits Severity: 3

443/tcp | 465/tcp | 995/tcp

Description

The TLS server uses a Diffie-Hellman group with a prime modulus of less than 2048 bits in length.  
 Current estimates are that that an academic team can break a 768-bit prime and that a state-level actor  
 can break a 1024-bit prime.

Solution

Please refer to this  
guide to deploying Diffie-Hellman for TLS  
https://weakdh.org/sysadmin.html

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:N/I:P/A:N

References Links

https://weakdh.org/

Pci

2, pass

Tag

Network

## TLS/SSL Server Is Using Commonly Used Prime Numbers Severity: 3

443/tcp | 465/tcp | 995/tcp

Description

The server is using a common or default prime number as a parameter during the Diffie-Hellman key exchange.  
 This makes the secure session vulnerable to a precomputation attack. An attacker can spend a significant amount  
 of time to generate a lookup/rainbow table for a particular prime number. This lookup table can then be used to obtain  
 the shared secret for the handshake and decrypt the session.

Solution

Configure the server to use a randomly generated Diffie-Hellman group. It's recommend that you generate a  
 2048-bit group. The simplest way of generating a new group is to use OpenSSL:  
openssl dhparam -out dhparams.pem 2048  
To use the DH parameters in newer versions of Apache (2.4.8 and newer) and OpenSSL 1.0.2 or later, you can directly specify your DH params file as follows:  
SSLOpenSSLConfCmd DHParameters "{path to dhparams.pem}"  
If you are using Apache with LibreSSL, or Apache 2.4.7 and OpenSSL 0.9.8a or later, you can append the DHparams you generated earlier to the end of your certificate file and reload the configuration.  
For other products see  
the remediation steps suggested by the original researchers.  
https://weakdh.org/sysadmin.html

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:N/I:P/A:N

References Links

https://weakdh.org/

https://www.openssl.org/docs/manmaster/apps/dhparam.html

Pci

2, pass

Tag

Network

## SHA-1-based Signature in TLS/SSL Server X.509 Certificate Severity: 3

443/tcp

Description

The SHA-1 hashing algorithm has known weaknesses that expose it to collision attacks, which  
 may allow an attacker to generate additional X.509 digital certificates with the same signature  
 as an original.

Solution

Stop using signature algorithms relying on SHA-1, such as "SHA1withRSA",  
 when signing X.509 certificates. Instead, use the  
 SHA-2 family (SHA-224, SHA-256, SHA-384, and SHA-512).

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:N/I:P/A:N

References Links

https://technet.microsoft.com/en-us/library/security/2880823.aspx

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

http://googleonlinesecurity.blogspot.co.uk/2014/09/gradually-sunsetting-sha-1.html

https://www.schneier.com/blog/archives/2005/02/cryptanalysis\_o.html

Pci

2, pass

Tag

Network, Web

## Untrusted TLS/SSL server X.509 certificate Severity: 6

443/tcp | 465/tcp | 995/tcp

Description

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted.  
 This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server  
 hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed  
 certificate is being used. The use of a self-signed certificate is not recommended since it could indicate  
 that a TLS/SSL man-in-the-middle attack is taking place

Solution

Ensure the common name (CN) reflects the name of the entity   
 presenting the certificate (e.g., the hostname).  
 If the certificate(s) or any of the chain certificate(s) have   
 expired or been revoked, obtain a new certificate from your   
 Certificate Authority (CA) by following their documentation.   
 If a self-signed certificate is being used, consider obtaining   
 a signed certificate from a CA.  
References:  
Mozilla: Connection Untrusted Error  
https://support.mozilla.org/en-US/kb/connection-untrusted-error-message  
SSLShopper: SSL Certificate Not Trusted Error  
https://www.sslshopper.com/ssl-certificate-not-trusted-error.html  
Windows/IIS certificate chain config  
https://support.microsoft.com/en-us/kb/954755  
Apache SSL config  
http://httpd.apache.org/docs/2.2/mod/mod\_ssl.html  
Nginx SSL config  
http://nginx.org/en/docs/http/configuring\_https\_servers.html  
CertificateChain.io  
https://certificatechain.io/

CVSS (Base Score)

5.8 AV:N/AC:M/Au:N/C:P/I:P/A:N

References Links

http://httpd.apache.org/docs/2.2/mod/mod\_ssl.html

http://nginx.org/en/docs/http/configuring\_https\_servers.html

https://support.microsoft.com/en-us/kb/954755

Pci

3, fail

Tag

Network

## TLS Server Supports TLS version 1.0 Severity: 4

443/tcp | 465/tcp | 995/tcp

Description

The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1  
 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of  
 TLS v1.1 and recommends TLS v1.2.

Solution

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References Links

https://www.pcisecuritystandards.org/documents/Migrating\_from\_SSL\_Early\_TLS\_Information%20Supplement\_v1.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Pci

3, fail

Tag

Network

## TLS Server Supports TLS version 1.1 Severity: 3

443/tcp

Description

The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1  
 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of  
 TLS v1.1 and recommends TLS v1.2.

Solution

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N

References Links

https://www.pcisecuritystandards.org/documents/Migrating\_from\_SSL\_Early\_TLS\_Information%20Supplement\_v1.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Pci

2, pass

Tag

Network

## Weak Cryptographic Key Severity: 3

443/tcp

Description

The key length used by a cryptographic algorithm determines the highest  
 security it can offer. Newly discovered theoretical attacks and hardware  
 advances constantly erode this security level over time. Taking this  
 into account, as of 2011, governmental, academic, and private  
 organizations providing guidance on cryptographic security, such as  
 the National Institute of Standards and Technology(http://www.nist.gov) European Network of Excellence in Cryptology II(http://www.ecrypt.eu.org) Symmetric key lengths of at least 80-112 bits. Elliptic curve key lengths of at least 160-224 bits. RSA key lengths of at least 1248-2048 bits.  
 In particular, the CA/Browser Forum Extended Validation (EV) Guidelines(http://www.cabforum.org/EV\_Certificate\_Guidelines.pdf) is within practical reach.(http://people.csail.mit.edu/tromer/papers/tromer-phd-dissertation-11pt.pdf) DSA key lengths of at least 2048 bits. Additionally, starting in 2014, the Certificate Authority/Browser Forum has mandated that 1024-bit RSA keys no  
 longer be supported for SSL certificates or code signing.

Solution

If the weak key is used in an X.509 certificate (for example for an HTTPS server),  
 generate a longer key and recreate the certificate.  
Please also refer to  
NIST's  
 recommendations on cryptographic algorithms and key lengths  
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

CVSS (Base Score)

3.2 AV:A/AC:H/Au:N/C:P/I:P/A:N

References Links

http://csrc.nist.gov/groups/ST/toolkit/key\_management.html

http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011\_2\_AlgoKatpdf.pdf

http://www.ecrypt.eu.org/documents/D.SPA.17.pdf

http://www.keylength.com

http://www.ssi.gouv.fr/IMG/pdf/RGS\_B\_1.pdf

http://www.symantec.com/page.jsp?id=1024-bit-certificate-support

Pci

2, pass

Tag

Network, Web

# 192.168.31.185

## OpenSSL Multiple Vulnerabilities -01 Mar16 (Windows) Severity: 10 (High)

general/tcp

Summary

This host is running OpenSSL and is prone  
 to multiple vulnerabilities.

Description

Installed version: 1.0.2e  
Fixed version: 1.0.2g  
  
Insight:  
Multiple flaws are due to,  
 - A double-free vulnerability in DSA code.  
 - A memory leak vulnerability in SRP database lookups using the   
 'SRP\_VBASE\_get\_by\_user' function.  
 - An integer overflow flaw in some 'BIGNUM' functions, leading to a NULL   
 pointer dereference or a heap-based memory corruption.  
 - An improper processing of format string in the 'BIO\_\*printf' functions.  
 - A side channel attack on modular exponentiation.  
 - The 'doapr\_outch' function in 'crypto/bio/b\_print.c' script does not verify  
 the success of a certain memory allocation

Solution

Upgrade to OpenSSL 1.0.1s or 1.0.2g or   
 later. For updates refer to https://www.openssl.org

CVSS (Base Score)

10.0 AV:N/AC:L/Au:N/C:C/I:C/A:C

References

**CVE**

CVE-2016-0705

CVE-2016-0798

CVE-2016-0797

CVE-2016-0799

CVE-2016-0702

CVE-2016-2842

**DFN-CERT**

DFN-CERT-2016-1401

DFN-CERT-2016-1389

DFN-CERT-2016-1245

DFN-CERT-2016-1175

DFN-CERT-2016-1174

DFN-CERT-2016-1103

DFN-CERT-2016-1026

DFN-CERT-2016-0951

DFN-CERT-2016-0890

DFN-CERT-2016-0841

DFN-CERT-2016-0815

DFN-CERT-2016-0803

DFN-CERT-2016-0789

DFN-CERT-2016-0765

DFN-CERT-2016-0699

DFN-CERT-2016-0698

DFN-CERT-2016-0644

DFN-CERT-2016-0499

DFN-CERT-2016-0496

DFN-CERT-2016-0465

DFN-CERT-2016-0459

DFN-CERT-2016-0453

DFN-CERT-2016-0403

DFN-CERT-2016-0388

DFN-CERT-2016-0360

DFN-CERT-2016-0359

DFN-CERT-2016-0357

References Links

https://www.openssl.org/news/secadv/20160301.txt

Impact

Affected Software/OS:  
OpenSSL versions 1.0.1 before 1.0.1s   
 and 1.0.2 before 1.0.2g on Windows.

## OpenSSL Multiple Vulnerabilities -01 May16 (Windows) Severity: 7.8 (High)

general/tcp

Summary

This host is running OpenSSL and is prone  
 to multiple vulnerabilities.

Description

Installed version: 1.0.2e  
Fixed version: 1.0.2h  
  
Insight:  
Multiple flaws are due to,  
 - An integer overflow in the EVP\_EncryptUpdate function in crypto/evp/evp\_enc.c  
 script in OpenSSL.  
 - An integer overflow in the EVP\_EncodeUpdate function in crypto/evp/encode.c  
 script in OpenSSL.  
 - An error in the 'asn1\_d2i\_read\_bio' function in crypto/asn1/a\_d2i\_fp.c script  
 in the ASN.1 BIO implementation in OpenSSL.  
 - An error in 'X509\_NAME\_oneline' function in crypto/x509/x509\_obj.c in OpenSSL.  
 - A MITM attacker can use a padding oracle attack to decrypt traffic  
 when the connection uses an AES CBC cipher and the server support AES-NI.

Solution

Upgrade to OpenSSL 1.0.1t or 1.0.2h or   
 later. For updates refer to https://www.openssl.org

CVSS (Base Score)

7.8 AV:N/AC:L/Au:N/C:N/I:N/A:C

References

**CVE**

CVE-2016-2176

CVE-2016-2109

CVE-2016-2106

CVE-2016-2107

CVE-2016-2105

**DFN-CERT**

DFN-CERT-2016-1401

DFN-CERT-2016-1372

DFN-CERT-2016-1175

DFN-CERT-2016-1174

DFN-CERT-2016-1169

DFN-CERT-2016-1166

DFN-CERT-2016-1160

DFN-CERT-2016-1103

DFN-CERT-2016-1092

DFN-CERT-2016-1091

DFN-CERT-2016-1026

DFN-CERT-2016-0951

DFN-CERT-2016-0815

DFN-CERT-2016-0765

DFN-CERT-2016-0740

DFN-CERT-2016-0702

References Links

https://www.openssl.org/news/secadv/20160503.txt

https://mta.openssl.org/pipermail/openssl-announce/2016-April/000069.html

Impact

Affected Software/OS:  
OpenSSL versions 1.0.1 before 1.0.1t   
 and 1.0.2 before 1.0.2h on Windows.

## OpenSSL Multiple Vulnerabilities -19 Jun16 (Windows) Severity: 7.5 (High)

general/tcp

Summary

This host is running OpenSSL and is prone to multiple vulnerabilities.

Description

Installed version: 1.0.2e  
Fixed version: Ask vendor  
  
Insight:  
Multiple flaws are due to ,   
1. Incorrectly using of pointer arithmetic for heap-buffer boundary checks which might allow remote attackers to cause a denial of service or possibly   
 have unspecified other impact by leveraging unexpected malloc behavior, related to s3\_srvr.c, ssl\_sess.c, and t1\_lib.c .  
2. Inproperly use of constant-time operations in crypto/dsa/dsa\_oss.c which allow local users to breach the DSA private key.

Solution

For undefined pointer arithmetic vulnerability, there is a fix available for OpenSSL 1.0.2 and OpenSSL 1.0.1. Refer to   
https://www.openssl.org/blog/blog/2016/06/27/undefined-pointer-arithmetic/.   
 To prevent DSA private key breach, a fix is available at https://git.openssl.org/?p

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:N/A:P

References

**CVE**

CVE-2016-2177

CVE-2016-2178

**DFN-CERT**

DFN-CERT-2016-1136

References Links

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2177

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2178

Impact

Affected Software/OS:  
 Openssl:1.0.2h and previous versions

## phpinfo() output accessible Severity: 7.5 (High)

80/tcp

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 times  
 left in webserver directory after completion.

Description

The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker:  
  
http://192.168.31.185/dashboard/phpinfo.php

Solution

Delete them or restrict access to the listened files.

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

## PHP Multiple Vulnerabilities-05 July16 (Windows) Severity: 7.5 (High)

80/tcp | 443/tcp

Summary

This host is installed with php and is prone  
 to multiple vulnerabilities.

Description

Installed version: 7.0.8  
Fixed version: 7.0.9  
  
Insight:  
Multiple flaws are due to  
 - An integer overflow in the 'php\_stream\_zip\_opener' function in  
 'ext/zip/zip\_stream.c' script.  
 - An integer signedness error in the 'simplestring\_addn' function in  
 'simplestring.c' in xmlrpc-epi.  
 - The 'ext/snmp/snmp.c' script improperly interacts with the unserialize   
 implementation and garbage collection.  
 - The 'locale\_accept\_from\_http' function in 'ext/intl/locale/locale\_methods.c'  
 script does not properly restrict calls to the ICU 'uloc\_acceptLanguageFromHTTP'   
 function.  
 - An error in the 'exif\_process\_user\_comment' function in 'ext/exif/exif.c'  
 script.  
 - An error in the 'exif\_process\_IFD\_in\_MAKERNOTE' function in 'ext/exif/exif.c'  
 script.  
 - The 'ext/session/session.c' does not properly maintain a certain hash data  
 structure.  
 - An integer overflow in the 'virtual\_file\_ex' function in  
 'TSRM/tsrm\_virtual\_cwd.c' script.  
 - An error in the 'php\_url\_parse\_ex' function in 'ext/standard/url.c' script.

Solution

Upgrade to php version 5.5.38, or 5.6.24,  
 or 7.0.9, or later.  
 For updates refer to http://www.php.net

CVSS (Base Score)

7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

References

**CVE**

CVE-2016-6288

CVE-2016-6289

CVE-2016-6290

CVE-2016-6291

CVE-2016-6292

CVE-2016-6294

CVE-2016-6295

CVE-2016-6296

CVE-2016-6297

**BID**

92111

92074

92097

92073

92078

92115

92094

92095

92099

**DFN-CERT**

DFN-CERT-2016-1335

DFN-CERT-2016-1326

DFN-CERT-2016-1310

DFN-CERT-2016-1253

DFN-CERT-2016-1179

References Links

http://php.net/ChangeLog-5.php

http://php.net/ChangeLog-7.php

http://openwall.com/lists/oss-security/2016/07/24/2

Impact

Affected Software/OS:  
PHP versions before 5.5.38, 5.6.x before  
 5.6.24, and 7.x before 7.0.9 on Windows

## http TRACE XSS attack Severity: 5.8 (Medium)

80/tcp | 443/tcp

Summary

Debugging functions are enabled on the remote HTTP server.  
  
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK  
are HTTP methods which are used to debug web server connections.   
  
It has been shown that servers supporting this method are subject to  
cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when  
used in conjunction with various weaknesses in browsers.   
  
An attacker may use this flaw to trick your legitimate web users to give  
him their credentials.

Solution

Disable these methods.  
  
   
Add the following lines for each virtual host in your configuration file :  
  
 RewriteEngine on  
 RewriteCond %{REQUEST\_METHOD} ^(TRACE|TRACK)  
 RewriteRule .\* - [F]  
  
See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable

CVSS (Base Score)

5.8 AV:N/AC:M/Au:N/C:P/I:P/A:N

References

**CVE**

CVE-2004-2320

CVE-2003-1567

**BID**

9506

9561

11604

**CERT-Bund**

CB-K14/0981

**DFN-CERT**

DFN-CERT-2014-1018

References Links

http://www.kb.cert.org/vuls/id/867593

## phpMyAdmin Multiple Vulnerabilities -01 May16 (Windows) Severity: 5.8 (Medium)

80/tcp | 443/tcp

Summary

This host is installed with phpMyAdmin  
 and is prone to multiple vulnerabilities.

Description

Installed version: 4.5.1  
Fixed version: 4.5.5.1  
  
Insight:  
Multiple flaws are due to,   
 - An input validation error in format function in   
 'libraries/sql-parser/src/Utils/Error.php' script in the SQL parser.   
 - The checkHTTP function in 'libraries/Config.class.php' script   
 does not verify X.509 certificates from api.github.com SSL servers.

Solution

Upgrade to phpMyAdmin version 4.5.5.1 or   
 later or apply patch from the link mentioned in reference.  
 For updates refer to https://www.phpmyadmin.net

CVSS (Base Score)

5.8 AV:N/AC:M/Au:N/C:P/I:P/A:N

References

**CVE**

CVE-2016-2559

CVE-2016-2562

**DFN-CERT**

DFN-CERT-2016-0355

References Links

https://www.phpmyadmin.net/security/PMASA-2016-10

https://www.phpmyadmin.net/security/PMASA-2016-13

Impact

Affected Software/OS:  
phpMyAdmin versions 4.5.x before 4.5.5.1  
 on Windows.

## PHP Man-in-the-Middle Attack Vulnerability July16 (Windows) Severity: 5.1 (Medium)

80/tcp | 443/tcp

Summary

This host is installed with php and is prone  
 to Man-in-the-middle attack vulnerability.

Description

Installed version: 7.0.8  
Fixed version: 7.0.9  
  
Insight:  
The web servers running in a CGI or   
 CGI-like context may assign client request Proxy header values to internal   
 HTTP\_PROXY environment variables and 'HTTP\_PROXY' is improperly trusted by some   
 PHP libraries and applications and flaw exist in the gdImageCropThreshold  
 function in 'gd\_crop.c' in the GD Graphics Library.

Solution

Upgrade to php version 7.0.9 or later.  
 For updates refer to http://www.php.net

CVSS (Base Score)

5.1 AV:N/AC:H/Au:N/C:P/I:P/A:P

References

**CVE**

CVE-2016-5385

CVE-2016-6128

**BID**

91821

91509

**DFN-CERT**

DFN-CERT-2016-1367

DFN-CERT-2016-1326

DFN-CERT-2016-1253

DFN-CERT-2016-1184

DFN-CERT-2016-1179

DFN-CERT-2016-1178

DFN-CERT-2016-1157

DFN-CERT-2016-1144

DFN-CERT-2016-1110

References Links

http://www.kb.cert.org/vuls/id/797896

https://bugs.php.net/bug.php?id=72573

https://bugs.php.net/bug.php?id=72494

Impact

Affected Software/OS:  
PHP versions prior to 7.0.9 on Windows

## Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Windows) Severity: 5.1 (Medium)

80/tcp | 443/tcp

Summary

This host is installed with Apache HTTP Server  
 and is prone to man-in-the-middle attack vulnerability.

Description

Installed version: 2.4.18  
Fixed version: 2.4.24  
  
Insight:  
The flaw is due to 'CGI Servlet' does not  
 protect applications from the presence of untrusted client data in the  
 'HTTP\_PROXY' environment variable.

Solution

Upgrade to version 2.4.24, or 2.2.32, or newer.  
 For updates refer http://www.apache.org

CVSS (Base Score)

5.1 AV:N/AC:H/Au:N/C:P/I:P/A:P

References

**CVE**

CVE-2016-5387

**BID**

91816

**DFN-CERT**

DFN-CERT-2016-1372

DFN-CERT-2016-1175

DFN-CERT-2016-1162

DFN-CERT-2016-1153

References Links

https://www.apache.org/security/asf-httpoxy-response.txt

Impact

Affected Software/OS:  
Apache HTTP Server through 2.4.23 on Windows  
 ----  
 NOTE: Apache HTTP Server 2.2.32 is not vulnerable  
 ----

## Apache /server-status accessible Severity: 5 (Medium)

80/tcp | 443/tcp

Summary

Leak of information in Apache.

Description

Vulnerable url: http://192.168.31.185/server-status  
Vulnerable url: https://192.168.31.185/server-status  
  
Insight:  
server-status is a built-in Apache HTTP Server handler used to  
 retrieve the server's status report.

Solution

If you don't use this feature, comment the appropriate section in  
 your httpd.conf file. If you really need it, limit its access to the administrator's machine.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

Impact

Requesting the URI /server-status gives information about  
 the currently running Apache.Affected Software/OS:  
All Apache version.

## Apache /server-info accessible Severity: 5 (Medium)

80/tcp | 443/tcp

Summary

Requesting the URI /server-info gives information about  
 your Apache configuration.

Description

Vulnerable url: http://192.168.31.185/server-info  
Vulnerable url: https://192.168.31.185/server-info  
  
Insight:  
server-info is a built-in Apache HTTP Server handler used to  
 retrieve the server's status report.

Solution

If you don't use this feature, comment the appropriate section in  
 your httpd.conf file. If you really need it, limit its access to the administrator's machine.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

Impact

Requesting the URI /server-info gives information about  
 the currently running Apache.Affected Software/OS:  
All Apache version.

## phpMyAdmin Multiple Vulnerabilities -02 Feb16 Severity: 5 (Medium)

80/tcp | 443/tcp

Summary

This host is installed with phpMyAdmin  
 and is prone to multiple vulnerabilities.

Description

Vulnerable url: http://192.168.31.185/phpmyadmin/libraries/sql-parser/autoload.php  
Vulnerable url: https://192.168.31.185/phpmyadmin/libraries/sql-parser/autoload.php  
  
Insight:  
Multiple flaws are due to:   
 - recommended setting of the PHP configuration directive display\_errors is   
 set to on, which is against the recommendations given in the PHP manual   
 for a production server.  
 - Insufficient validation of user supplied input via SQL query in the   
 SQL editor

Solution

Upgrade to phpMyAdmin version 4.5.4 or  
 or later or apply patch from the link mentioned in reference.  
 For updates refer to https://www.phpmyadmin.net

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2016-2044

CVE-2016-2045

**BID**

82104

82100

**CERT-Bund**

CB-K16/0149

**DFN-CERT**

DFN-CERT-2016-0161

References Links

https://www.phpmyadmin.net/security/PMASA-2016-9

https://www.phpmyadmin.net/security/PMASA-2016-8

Impact

Affected Software/OS:  
phpMyAdmin versions 4.5.x before 4.5.4

## DCE Services Enumeration Severity: 5 (Medium)

135/tcp

Summary

Distributed Computing Environment (DCE) services running on the remote host   
can be enumerated by connecting on port 135 and doing the appropriate queries.   
  
An attacker may use this fact to gain more knowledge  
about the remote host.

Solution

filter incoming traffic to this port.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

## DCE Services Enumeration Severity: 5 (Medium)

135/tcp

Summary

Distributed Computing Environment (DCE) services running on the remote host   
can be enumerated by connecting on port 135 and doing the appropriate queries.   
  
An attacker may use this fact to gain more knowledge  
about the remote host.

Description

Distributed Computing Environment (DCE) services running on the remote host  
can be enumerated by connecting on port 135 and doing the appropriate queries.  
  
An attacker may use this fact to gain more knowledge  
about the remote host.  
  
  
Here is the list of DCE services running on this host:  
  
Port: 49664/tcp  
  
 UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49664]  
  
Port: 49665/tcp  
  
 UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49665]  
 Annotation: Event log TCPIP  
  
 UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49665]  
 Annotation: DHCP Client LRPC Endpoint  
  
 UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49665]  
 Annotation: DHCPv6 Client LRPC Endpoint  
  
 UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49665]  
 Annotation: Security Center  
  
Port: 49666/tcp  
  
 UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
  
 UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
  
 UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: UserMgrCli  
  
 UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: UserMgrCli  
  
 UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: IP Transition Configuration endpoint  
  
 UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: Proxy Manager provider server endpoint  
  
 UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: Adh APIs  
  
 UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: Proxy Manager client server endpoint  
  
 UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: XactSrv service  
  
 UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: IdSegSrv service  
  
 UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: AppInfo  
  
 UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: AppInfo  
  
 UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: AppInfo  
  
 UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: AppInfo  
  
 UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: AppInfo  
  
 UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
  
 UUID: 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49666]  
 Annotation: Vpn APIs  
  
Port: 49667/tcp  
  
 UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49667]  
 Named pipe : spoolss  
 Win32 service or process : spoolsv.exe  
 Description : Spooler service  
  
 UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49667]  
  
 UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49667]  
  
 UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49667]  
  
 UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49667]  
  
Port: 49669/tcp  
  
 UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49669]  
  
Port: 49679/tcp  
  
 UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1  
 Endpoint: ncacn\_ip\_tcp:192.168.31.185[49679]  
 Named pipe : lsass  
 Win32 service or process : lsass.exe  
 Description : SAM access  
  
  
  
Solution : filter incoming traffic to this port(s).

Solution

filter incoming traffic to this port.

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

## phpMyAdmin Information Disclosure Vulnerability Severity: 5 (Medium)

443/tcp | 80/tcp

Summary

This host is installed with phpMyAdmin  
 and is prone to information disclosure vulnerability.

Description

Vulnerable url: https://192.168.31.185/phpmyadmin/libraries/config/messages.inc.php  
Vulnerable url: http://192.168.31.185/phpmyadmin/libraries/config/messages.inc.php  
  
Insight:  
The flaw is due to recommended setting of  
 the PHP configuration directive display\_errors is set to on, which is against  
 the recommendations given in the PHP manual for a production server.

Solution

Upgrade to phpMyAdmin version 4.0.10.12 or  
 4.4.15.2 or 4.5.3.1 or later or apply patch from the link mentioned in reference.  
 For updates refer to https://www.phpmyadmin.net

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2015-8669

**BID**

79691

**CERT-Bund**

CB-K15/1890

**DFN-CERT**

DFN-CERT-2015-1997

References Links

https://www.phpmyadmin.net/security/PMASA-2015-6

https://github.com/phpmyadmin/phpmyadmin/commit/c4d649325b25139d7c097e56e2e46cc7187fae45

Impact

Affected Software/OS:  
phpMyAdmin versions 4.0.x prior to 4.0.10.12,  
 4.4.x prior to 4.4.15.2 and 4.5.x prior to 4.5.3.1

## phpMyAdmin Multiple Vulnerabilities -01 Feb16 Severity: 5 (Medium)

443/tcp | 80/tcp

Summary

This host is installed with phpMyAdmin  
 and is prone to multiple vulnerabilities.

Description

Vulnerable url: https://192.168.31.185/phpmyadmin/setup/lib/common.inc.php  
Vulnerable url: http://192.168.31.185/phpmyadmin/setup/lib/common.inc.php  
  
Insight:  
Multiple flaws are due to,   
 - The recommended setting of the PHP configuration directive display\_errors is   
 set to on, which is against the recommendations given in the PHP manual   
 for a production server.  
 - The XSRF/CSRF token is generated with a weak algorithm using functions   
 that do not return cryptographically secure values.  
 - An insufficient validation of user supplied input via parameters   
 table name, SET value, hostname header and search query.   
 - The password suggestion functionality uses 'Math.random' function which does  
 not provide cryptographically secure random numbers.  
 - The 'libraries/common.inc.php' script does not use a constant-time algorithm  
 for comparing CSRF tokens.

Solution

Upgrade to phpMyAdmin version 4.0.10.13 or   
 4.4.15.3 or 4.5.4 or later or apply patch from the link mentioned in reference.  
 For updates refer to https://www.phpmyadmin.net

CVSS (Base Score)

5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2016-2038

CVE-2016-2039

CVE-2016-2040

CVE-2016-2041

CVE-2016-1927

**BID**

82075

81210

82077

82084

82076

**CERT-Bund**

CB-K16/0149

**DFN-CERT**

DFN-CERT-2016-1188

DFN-CERT-2016-0161

References Links

https://www.phpmyadmin.net/security/PMASA-2016-4

https://www.phpmyadmin.net/security/PMASA-2016-5

https://www.phpmyadmin.net/security/PMASA-2016-3

https://www.phpmyadmin.net/security/PMASA-2016-2

https://www.phpmyadmin.net/security/PMASA-2016-1

Impact

Affected Software/OS:  
phpMyAdmin versions 4.0.x prior to 4.0.10.13,   
 4.4.x prior to 4.4.15.3 and 4.5.x prior to 4.5.4

## OpenSSL Multiple MitM Attack Vulnerabilities (Windows) Severity: 4.3 (Medium)

general/tcp

Summary

This host is running OpenSSL and is prone  
 to multiple man-in-the-middle (MitM) attack vulnerabilities.

Description

Installed version: 1.0.2e  
Fixed version: 1.0.2f  
  
Insight:  
Multiple flaws found,  
 - The way malicious SSL/TLS clients could negotiate SSLv2 ciphers that have  
 been disabled on the server.  
 - When a DHE\_EXPORT ciphersuite is enabled on a server but not on a client,  
 does not properly convey a DHE\_EXPORT choice.

Solution

Upgrade to OpenSSL 1.0.1r or 1.0.2f or later.  
 For updates refer https://www.openssl.org

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2015-3197

CVE-2015-4000

**CERT-Bund**

CB-K16/0168

CB-K16/0146

CB-K16/0121

CB-K16/0090

CB-K16/0030

CB-K15/1591

CB-K15/1550

CB-K15/1517

CB-K15/1464

CB-K15/1442

CB-K15/1334

CB-K15/1269

CB-K15/1136

CB-K15/1090

CB-K15/1059

CB-K15/1022

CB-K15/1015

CB-K15/0964

CB-K15/0932

CB-K15/0927

CB-K15/0926

CB-K15/0907

CB-K15/0901

CB-K15/0896

CB-K15/0877

CB-K15/0834

CB-K15/0802

CB-K15/0733

**DFN-CERT**

DFN-CERT-2016-1174

DFN-CERT-2016-1168

DFN-CERT-2016-0665

DFN-CERT-2016-0647

DFN-CERT-2016-0644

DFN-CERT-2016-0642

DFN-CERT-2016-0638

DFN-CERT-2016-0495

DFN-CERT-2016-0465

DFN-CERT-2016-0459

DFN-CERT-2016-0453

DFN-CERT-2016-0415

DFN-CERT-2016-0403

DFN-CERT-2016-0388

DFN-CERT-2016-0360

DFN-CERT-2016-0359

DFN-CERT-2016-0184

DFN-CERT-2016-0166

DFN-CERT-2016-0135

DFN-CERT-2016-0101

DFN-CERT-2016-0035

DFN-CERT-2015-1679

DFN-CERT-2015-1632

DFN-CERT-2015-1608

DFN-CERT-2015-1542

DFN-CERT-2015-1518

DFN-CERT-2015-1406

DFN-CERT-2015-1341

DFN-CERT-2015-1194

DFN-CERT-2015-1144

DFN-CERT-2015-1113

DFN-CERT-2015-1078

DFN-CERT-2015-1067

DFN-CERT-2015-1016

DFN-CERT-2015-0980

DFN-CERT-2015-0977

DFN-CERT-2015-0976

DFN-CERT-2015-0960

DFN-CERT-2015-0956

DFN-CERT-2015-0944

DFN-CERT-2015-0925

DFN-CERT-2015-0879

DFN-CERT-2015-0844

DFN-CERT-2015-0737

References Links

https://www.openssl.org/news/secadv/20160128.txt

Impact

Affected Software/OS:  
OpenSSL versions 1.0.1x before 1.0.1r and  
 1.0.2x before 1.0.2f on Windows.

## OpenSSL SSLv2 DROWN Attack Vulnerability (Windows) Severity: 4.3 (Medium)

general/tcp

Summary

This host is running OpenSSL and is prone  
 to DROWN attack vulnerability.

Description

Installed version: 1.0.2e  
Fixed version: 1.0.2g  
  
Insight:  
The flaw is due a padding oracle flaw found   
 in the SSLv2 protocol, so that by exploiting the server's support of SSLv2,   
 an attacker can decrypt properly secured TLS traffic.

Solution

Upgrade to OpenSSL 1.0.1s or 1.0.2g or   
 later. For updates refer https://www.openssl.org

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2016-0800

**DFN-CERT**

DFN-CERT-2016-1216

DFN-CERT-2016-1174

DFN-CERT-2016-1168

DFN-CERT-2016-0841

DFN-CERT-2016-0644

DFN-CERT-2016-0496

DFN-CERT-2016-0495

DFN-CERT-2016-0465

DFN-CERT-2016-0459

DFN-CERT-2016-0453

DFN-CERT-2016-0451

DFN-CERT-2016-0415

DFN-CERT-2016-0403

DFN-CERT-2016-0388

DFN-CERT-2016-0360

DFN-CERT-2016-0359

DFN-CERT-2016-0357

References Links

https://www.openssl.org/news/secadv/20160301.txt

https://drownattack.com/drown-attack-paper.pdf

https://answers.uchicago.edu/page.php?id=61323

http://arstechnica.com/security/2016/03/more-than-13-million-https-websites-imperiled-by-new-decryption-attack

Impact

Affected Software/OS:  
OpenSSL versions before 1.0.1s and 1.0.2   
 before 1.0.2g on Windows.

## phpMyAdmin Multiple XSS Vulnerabilities -02 May16 (Windows) Severity: 4.3 (Medium)

80/tcp | 443/tcp

Summary

This host is installed with phpMyAdmin  
 and is prone to multiple xss vulnerabilities.

Description

Installed version: 4.5.1  
Fixed version: 4.5.5.1  
  
Insight:  
Multiple flaws are due to,   
 - An input validation error via Host HTTP header, related to   
 'libraries/Config.class.php' script.  
 - An input validation error via JSON data, related to 'file\_echo.php' script.  
 - An input validation error related to SQL query in 'js/functions.js script'.  
 - An input validation error via the initial parameter to   
 'libraries/server\_privileges.lib.php' script in the user accounts page.  
 - An input validation error via a parameter to   
 'libraries/controllers/TableSearchController.class.php' script in the   
 zoom search page.

Solution

Upgrade to phpMyAdmin version 4.0.10.15 or  
 4.4.15.5 or 4.5.5.1 or later or apply patch from the link mentioned in reference.  
 For updates refer to https://www.phpmyadmin.net

CVSS (Base Score)

4.3 AV:N/AC:M/Au:N/C:N/I:P/A:N

References

**CVE**

CVE-2016-2560

**DFN-CERT**

DFN-CERT-2016-1188

DFN-CERT-2016-0355

References Links

https://www.phpmyadmin.net/security/PMASA-2016-11

Impact

Affected Software/OS:  
phpMyAdmin versions 4.0.x before 4.0.10.15,   
 4.4.x before 4.4.15.5, and 4.5.x before 4.5.5.1 on Windows.

## phpMyAdmin Multiple XSS Vulnerabilities -01 May16 (Windows) Severity: 3.5 (Low)

80/tcp | 443/tcp

Summary

This host is installed with phpMyAdmin  
 and is prone to multiple xss vulnerabilities.

Description

Installed version: 4.5.1  
Fixed version: 4.5.5.1  
  
Insight:  
Multiple flaws are due to,   
 - An input validation error via table/column name in database normalization   
 page.  
 - An input validation error in 'templates/database/structure/sortable\_header.phtml'   
 script in the database structure page.  
 - An input validation error in 'db\_central\_columns.php' script in the  
 central columns page.  
 - An input validation error in 'normalization.php' script.

Solution

Upgrade to phpMyAdmin version 4.4.15.5 or   
 4.5.5.1 or later or apply patch from the link mentioned in reference.  
 For updates refer to https://www.phpmyadmin.net

CVSS (Base Score)

3.5 AV:N/AC:M/Au:S/C:N/I:P/A:N

References

**CVE**

CVE-2016-2561

**DFN-CERT**

DFN-CERT-2016-1188

DFN-CERT-2016-0355

References Links

https://www.phpmyadmin.net/security/PMASA-2016-12

Impact

Affected Software/OS:  
phpMyAdmin versions 4.4.x before 4.4.15.5   
 and 4.5.x before 4.5.5.1 on Windows.

## OpenSSL 'Diffie-Hellman small subgroups' MitM Attack Vulnerability (Windows) Severity: 2.6 (Low)

general/tcp

Summary

This host is running OpenSSL and is prone  
 to man-in-the-middle (MitM) attack vulnerability.

Description

Installed version: 1.0.2e  
Fixed version: 1.0.2f  
  
Insight:  
The flaw exists as the primes used in X9.42 style  
 parameter files may not be safe. When an application is using Diffie-Hellman  
 configured with parameters based on primes that are not safe then an attacker  
 could use this fact to find a peer's private DH exponent.

Solution

Upgrade to OpenSSL 1.0.2f or later. For  
 updates refer https://www.openssl.org

CVSS (Base Score)

2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N

References

**CVE**

CVE-2016-0701

**CERT-Bund**

CB-K16/0146

**DFN-CERT**

DFN-CERT-2016-0166

References Links

https://www.openssl.org/news/secadv/20160128.txt

Impact

Affected Software/OS:  
OpenSSL versions 1.0.2x before 1.0.2f on  
 Windows.

## OS Detection Severity: 0

general/tcp

Summary

This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.

Description

Best matching OS:  
cpe:/o:microsoft:windows  
Found by NVT 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)  
  
Other OS detections (in order of reliability):  
OS: cpe:/h:hp:jetdirect found by 1.3.6.1.4.1.25623.1.0.102002 (Detects remote operating system version)

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Traceroute Severity: 0

general/tcp

Summary

A traceroute from the scanning server to the target system was  
conducted. This traceroute is provided primarily for informational  
value only. In the vast majority of cases, it does not represent a  
vulnerability. However, if the displayed traceroute contains any  
private addresses that should not have been publicly visible, then you  
have an issue you need to correct.

Description

Here is the route from 10.0.2.15 to 192.168.31.185:  
  
10.0.2.15  
192.168.31.185

Solution

Block unwanted packets from escaping your network.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## OpenSSL Remote Version Detection Severity: 0

general/tcp

Summary

Detection of installed version of  
 OpenSSL.  
  
 This script sends HTTP GET request and try to get the version from the  
 response, and sets the result in KB.

Description

Detected OpenSSL  
Version: 1.0.2e  
Location: /  
CPE: cpe:/a:openssl:openssl:1.0.2e  
  
Concluded from version identification result:  
"OpenSSL/1.0.2e" at port 443

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## SMB Remote Version Detection Severity: 0

general/tcp

Summary

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

Description

SMBv1 and SMBv2 are enabled on remote target

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## CPE Inventory Severity: 0

general/CPE-T

Summary

This routine uses information collected by other routines about  
CPE identities (http://cpe.mitre.org/) of operating systems, services and  
applications detected during the scan.

Description

192.168.31.185|cpe:/a:openssl:openssl:1.0.2e  
192.168.31.185|cpe:/a:apache:apr-util:1.5.4  
192.168.31.185|cpe:/a:apache:portable\_runtime:1.5.2  
192.168.31.185|cpe:/a:horde:horde\_groupware:1.2  
192.168.31.185|cpe:/a:horde:horde\_groupware:4.5.1  
192.168.31.185|cpe:/a:phpmyadmin:phpmyadmin:4.5.1  
192.168.31.185|cpe:/a:horde:chora:1.2  
192.168.31.185|cpe:/a:horde:chora:4.5.1  
192.168.31.185|cpe:/a:apache:http\_server:2.4.18  
192.168.31.185|cpe:/a:php:php:7.0.8  
192.168.31.185|cpe:/o:microsoft:windows

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## SMB Test Severity: 0

general/SMBClient

Summary

Test remote host SMB Functions

Description

Error getting SMB-Data -> SESSION SETUP FAILED: NT\_STATUS\_ACCESS\_DENIED

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## HTTP Server type and version Severity: 0

80/tcp | 443/tcp

Summary

This detects the HTTP Server's type and version.

Description

The remote web server type is :  
  
Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/7.0.8   
  
  
Solution : You can set the directive "ServerTokens Prod" to limit  
the information emanating from the server in its response headers.

Solution

Configure your server to use an alternate name like  
 'Wintendo httpD w/Dotmatrix display'  
 Be sure to remove common logos like apache\_pb.gif.  
 With Apache, you can set the directive 'ServerTokens Prod' to limit  
 the information emanating from the server in its response headers.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## DIRB (NASL wrapper) Severity: 0

80/tcp

Summary

This script uses DIRB to find directories and files on web  
 applications via brute forcing.

Description

This are the directories/files found with brute force:  
  
https://192.168.31.185:443/  
http://192.168.31.185:80/

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Web mirroring Severity: 0

80/tcp

Summary

This script makes a mirror of the remote web site  
 and extracts the list of CGIs that are used by the remote host.  
  
 It is suggested you allow a long-enough timeout value for  
 this test routine and also adjust the setting on  
 the number of pages to mirror.

Description

The following CGI have been discovered :  
  
Syntax : cginame (arguments [default value])  
  
/phpmyadmin/db\_operations.php (token [78387b6b32fe9f3361121bc185ca71b5] db [bwapp] server [1] )  
/phpmyadmin/doc/html/search.html (check\_keywords [yes] q [] area [default] )  
/phpmyadmin/phpmyadmin.css.php (nocache [5808682475ltr] )  
/phpmyadmin/themes/pmahomme/css/printview.css (v [4.5.1] )  
/dashboard/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
/dashboard/images/addons/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
/phpmyadmin/js/codemirror/addon/hint/show-hint.css (v [4.5.1] )  
/phpmyadmin/url.php (url [http%3A%2F%2Fdev.mysql.com%2Fdoc%2Frefman%2F5.7%2Fen%2Findex.html] )  
/phpmyadmin/navigation.php (token [78387b6b32fe9f3361121bc185ca71b5] ajax\_request [1] collation\_connection [utf8mb4\_unicode\_ci] lang [en] )  
/phpmyadmin/server\_databases.php (token [78387b6b32fe9f3361121bc185ca71b5] server [1] )  
/phpmyadmin/db\_structure.php (token [78387b6b32fe9f3361121bc185ca71b5] server [1] db [bwapp] )  
/phpmyadmin/index.php (phpMyAdmin [n9i3r50gpmih368ccu6k515kqhd6r67n] token [78387b6b32fe9f3361121bc185ca71b5] reload [1] collation\_connection [utf8mb4\_unicode\_ci] lang [en] )  
/dashboard/stylesheets/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
/dashboard/docs/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
/phpmyadmin/js/codemirror/addon/lint/lint.css (v [4.5.1] )  
/dashboard/images/screenshots/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
/dashboard/images/blog/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
/phpmyadmin/js/codemirror/lib/codemirror.css (v [4.5.1] )  
/dashboard/images/flags/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
  
The following directories have been discovered :  
  
/dashboard  
/dashboard/stylesheets  
/dashboard/images  
/phpmyadmin  
/icons  
/dashboard/images/addons  
/dashboard/images/blog  
/dashboard/images/flags  
/dashboard/images/screenshots  
/dashboard/docs  
/phpmyadmin/themes/pmahomme/jquery  
/phpmyadmin/js/codemirror/lib  
/phpmyadmin/js/codemirror/addon/hint  
/phpmyadmin/js/codemirror/addon/lint  
/phpmyadmin/themes/pmahomme/css  
/phpmyadmin/themes/pmahomme/img  
/phpmyadmin/themes  
/phpmyadmin/doc/html  
/dashboard/docs/images/backup-restore-mysql  
/dashboard/docs/images/transfer-files-ftp  
/dashboard/docs/images/configure-vhosts  
/dashboard/docs/images/configure-wildcard-subdomains  
/dashboard/docs/images/deploy-git-app  
/dashboard/docs/images/install-wordpress  
/dashboard/docs/images/reset-mysql-password  
/dashboard/docs/images/send-mail  
/dashboard/docs/images/use-sqlite  
/dashboard/docs/images/activate-use-xdebug  
/dashboard/docs/images/create-framework-project-zf1  
/dashboard/docs/images/create-framework-project-zf2  
/dashboard/docs/images/troubleshoot-apache  
/dashboard/docs/images/access-phpmyadmin-remotely  
/dashboard/docs/images/use-different-php-version  
/dashboard/docs/images/use-php-fcgi  
/phpmyadmin/doc/html/\_static  
/phpmyadmin/doc/html/\_sources  
  
  
Extraneous phpinfo() script found at /dashboard/phpinfo.php  
Directory index found at /dashboard/stylesheets/  
Directory index found at /dashboard/images/  
Directory index found at /dashboard/images/addons/  
Directory index found at /dashboard/images/blog/  
Directory index found at /dashboard/images/flags/  
Directory index found at /dashboard/images/screenshots/  
Directory index found at /dashboard/docs/

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Directory Scanner Severity: 0

80/tcp

Summary

This plugin attempts to determine the presence of various  
 common dirs on the remote web server

Description

The following directories were discovered:  
/cgi-bin, /webalizer, /error, /icons, /img, /server-info, /server-status  
  
While this is not, in and of itself, a bug, you should manually inspect   
these directories to ensure that they are in compliance with company  
security standards

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

References

**OWASP**

OWASP-CM-006

## Directories used for CGI Scanning Severity: 0

80/tcp

Summary

The script prints out the directories which  
 are used when CGI scanning is enabled.

Description

The following directories are used for CGI scanning:  
  
http://192.168.31.185/scripts  
http://192.168.31.185/cgi-bin  
http://192.168.31.185/img  
http://192.168.31.185/phpmyadmin/themes/pmahomme/jquery  
http://192.168.31.185/dashboard/images/screenshots  
http://192.168.31.185/dashboard/docs/images/configure-vhosts  
http://192.168.31.185/phpmyadmin/themes/pmahomme/img  
http://192.168.31.185/dashboard/docs/images/install-wordpress  
http://192.168.31.185/dashboard/docs/images/deploy-git-app  
http://192.168.31.185/dashboard/docs  
http://192.168.31.185/error  
http://192.168.31.185/server-info  
http://192.168.31.185/phpmyadmin/themes  
http://192.168.31.185/dashboard/docs/images/reset-mysql-password  
http://192.168.31.185/phpmyadmin/js/codemirror/addon/lint  
http://192.168.31.185/phpmyadmin/js/codemirror/addon/hint  
http://192.168.31.185/phpmyadmin/js/codemirror/lib  
http://192.168.31.185/dashboard/images/addons  
http://192.168.31.185/dashboard/docs/images/backup-restore-mysql  
http://192.168.31.185/dashboard/docs/images/transfer-files-ftp  
http://192.168.31.185/phpmyadmin/themes/pmahomme/css  
http://192.168.31.185/dashboard/images  
http://192.168.31.185/dashboard/docs/images/configure-wildcard-subdomains  
http://192.168.31.185/dashboard/docs/images/send-mail  
http://192.168.31.185/icons  
http://192.168.31.185/server-status  
http://192.168.31.185/dashboard/stylesheets  
http://192.168.31.185/dashboard/images/flags  
http://192.168.31.185/dashboard/docs/images/create-framework-project-zf1  
http://192.168.31.185/dashboard  
http://192.168.31.185/phpmyadmin  
http://192.168.31.185/dashboard/docs/images/use-sqlite  
http://192.168.31.185/dashboard/docs/images/create-framework-project-zf2  
http://192.168.31.185/phpmyadmin/doc/html/\_static  
http://192.168.31.185/dashboard/docs/images/access-phpmyadmin-remotely  
http://192.168.31.185/webalizer  
http://192.168.31.185/dashboard/images/blog  
http://192.168.31.185/dashboard/docs/images/activate-use-xdebug  
http://192.168.31.185/phpmyadmin/doc/html  
http://192.168.31.185/dashboard/docs/images/use-different-php-version  
http://192.168.31.185/dashboard/docs/images/troubleshoot-apache  
http://192.168.31.185/dashboard/docs/images/use-php-fcgi  
http://192.168.31.185/phpmyadmin/doc/html/\_sources  
http://192.168.31.185/

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Horde Detection Severity: 0

80/tcp | 443/tcp

Summary

The script sends a connection request to the server and attempts to  
extract the version number from the reply.

Description

Detected Horde  
Version: 1.2x of The Webalizer adds incremental run capability. Simply  
Location: /webalizer  
CPE: cpe:/a:horde:horde\_groupware:1.2  
  
Concluded from version identification result:  
Version 1.2x of The Webalizer adds incremental run capability. Simply

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## phpMyAdmin Detection Severity: 0

80/tcp | 443/tcp

Summary

Detection of phpMyAdmin.  
  
 The script sends a connection request to the server and attempts to  
 extract the version number from the reply.

Description

Detected phpMyAdmin  
Version: 4.5.1  
Location: /phpmyadmin  
CPE: cpe:/a:phpmyadmin:phpmyadmin:4.5.1  
  
Concluded from version identification result:  
phpMyAdmin 4.5.1  
  
  
(Possible unprotected /setup/ dir identified)

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## SMB on port 445 Severity: 0

139/tcp

Summary

This script detects wether port 445 and 139 are open and  
if thet are running SMB servers.

Description

An SMB server is running on this port

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## SSL Certificate - Self-Signed Certificate Detection Severity: 0

443/tcp

Summary

The SSL certificate on this port is self-signed.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

References Links

http://en.wikipedia.org/wiki/Self-signed\_certificate

## Services Severity: 0

443/tcp

Summary

This routine attempts to guess which  
service is running on the remote ports. 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.

Description

A TLScustom server answered on this port

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Services Severity: 0

443/tcp

Summary

This routine attempts to guess which  
service is running on the remote ports. 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.

Description

A web server is running on this port through SSL

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Checks for supported Non Weak SSL Ciphers Severity: 0

443/tcp

Summary

This Plugin report about supported Non Weak SSL Ciphers.

Description

Service does not support SSLv2 ciphers.  
  
Service does not support SSLv3 ciphers.  
  
Service supports TLSv1 ciphers.  
  
Service supports TLSv1.1 ciphers.  
  
Service supports TLSv1.2 ciphers.  
  
Medium ciphers offered by this service:  
 TLS1\_DHE\_RSA\_WITH\_SEED\_SHA  
 TLS1\_RSA\_WITH\_SEED\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_DES\_192\_CBC3\_SHA  
 TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_DHE\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_IDEA\_128\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_SEED\_SHA  
 TLS1\_RSA\_WITH\_SEED\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_DES\_192\_CBC3\_SHA  
 TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_DHE\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_IDEA\_128\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (custom override [Weak > Medium])  
 TLS\_1\_2\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (custom override [Weak > Medium])  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_CBC\_SHA  
  
No weak ciphers are supported by this service  
  
No non-ciphers are supported by this service

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Apache APR Version Detection (Remote) Severity: 0

443/tcp

Summary

This script tries to detects the installed version of Apache APR  
 from an exposed /server-info status page and sets the result in KB.

Description

Detected Apache APR  
Version: 1.5.2  
Location: 443/tcp  
CPE: cpe:/a:apache:portable\_runtime:1.5.2  
  
Concluded from version identification result:  
Server loaded APR Version:</strong> <tt>1.5.2</tt>

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Apache APR Version Detection (Remote) Severity: 0

443/tcp | 80/tcp

Summary

This script tries to detects the installed version of Apache APR  
 from an exposed /server-info status page and sets the result in KB.

Description

Detected Apache APR-Utils  
Version: 1.5.4  
Location: 443/tcp  
Location: 80/tcp  
CPE: cpe:/a:apache:apr-util:1.5.4  
  
Concluded from version identification result:  
Server loaded APU Version:</strong> <tt>1.5.4</tt>

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Chora Detection Severity: 0

443/tcp

Summary

This script detects whether the remote host is running Chora and  
extracts version numbers and locations of any instances found.   
  
Chora is a PHP-based interface to CVS repositories from the Horde  
Project. See http://www.horde.org/chora/ for more information.

Description

Summary:  
 Chora 1.2x of The Webalizer adds incremental run capability. Simply was detected on the remote host under the path /webalizer.   
  
Chora is a PHP-based interface to CVS repositories from the Horde  
Project. See http://www.horde.org/chora/ for more information.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Nikto (NASL wrapper) Severity: 0

443/tcp

Summary

This plugin uses nikto(1) to find weak CGI scripts  
and other known issues regarding web server security.  
See the preferences section for configuration options.

Description

Here is the Nikto report:  
- Nikto v2.1.6  
---------------------------------------------------------------------------  
+ Target IP: 192.168.31.185  
+ Target Hostname: 192.168.31.185  
+ Target Port: 443  
---------------------------------------------------------------------------  
+ SSL Info: Subject: /CN=localhost  
Ciphers: ECDHE-RSA-AES256-GCM-SHA384  
Issuer: /CN=localhost  
+ Start Time: 2016-08-31 15:49:20 (GMT0)  
---------------------------------------------------------------------------  
+ Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/7.0.8  
+ Retrieved x-powered-by header: PHP/7.0.8  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Root page / redirects to: https://192.168.31.185/dashboard/  
+ Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x78ae 0x51affc7a4c400   
+ Hostname '192.168.31.185' does not match certificate's names: localhost  
+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var, HTTP\_NOT\_FOUND.html.var  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources.  
+ OSVDB-3268: /img/: Directory indexing found.  
+ OSVDB-3092: /img/: This might be interesting...  
+ Uncommon header 'x-ob\_mode' found, with contents: 1  
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.  
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.  
+ OSVDB-3268: /icons/: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ /phpmyadmin/: phpMyAdmin directory found  
+ /server-status: Apache server-status interface found (pass protected)  
+ 8345 requests: 0 error(s) and 19 item(s) reported on remote host  
+ End Time: 2016-08-31 15:52:54 (GMT0) (214 seconds)  
---------------------------------------------------------------------------  
+ 1 host(s) tested

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## PHP Version Detection Severity: 0

443/tcp | 80/tcp

Summary

Detection of installed version of PHP.  
 This script sends HTTP GET request and try to get the version from the  
 response, and sets the result in KB.

Description

Detected PHP  
Version: 7.0.8  
Location: tcp/443  
Location: tcp/80  
CPE: cpe:/a:php:php:7.0.8  
  
Concluded from version identification result:  
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/7.0.8

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Check for SSL Ciphers Severity: 0

443/tcp

Summary

This routine search for SSL ciphers offered by a service.

Description

Service does not support SSLv2 ciphers.  
  
Service does not support SSLv3 ciphers.  
  
Service supports TLSv1 ciphers.  
  
Service supports TLSv1.1 ciphers.  
  
Service supports TLSv1.2 ciphers.  
  
Medium ciphers offered by this service:  
 TLS1\_DHE\_RSA\_WITH\_SEED\_SHA  
 TLS1\_RSA\_WITH\_SEED\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_DES\_192\_CBC3\_SHA  
 TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_DHE\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_IDEA\_128\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_SEED\_SHA  
 TLS1\_RSA\_WITH\_SEED\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_DES\_192\_CBC3\_SHA  
 TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_DHE\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_IDEA\_128\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (custom override [Weak > Medium])  
 TLS\_1\_2\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (custom override [Weak > Medium])  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_CBC\_SHA  
  
No weak ciphers are supported by this service  
  
No non-ciphers are supported by this service

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Apache Web Server Version Detection Severity: 0

443/tcp | 80/tcp

Summary

Detection of installed version of Apache Web Server  
  
 The script detects the version of Apache HTTP Server on remote host and sets the KB.

Description

Detected Apache  
Version: 2.4.18  
Location: 443/tcp  
Location: 80/tcp  
CPE: cpe:/a:apache:http\_server:2.4.18  
  
Concluded from version identification result:  
Server: Apache/2.4.18

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Check for SSL Medium Ciphers Severity: 0

443/tcp

Summary

This Plugin reports about SSL Medium Ciphers.

Description

Medium ciphers offered by this service:  
 TLS1\_DHE\_RSA\_WITH\_SEED\_SHA  
 TLS1\_RSA\_WITH\_SEED\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_DES\_192\_CBC3\_SHA  
 TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_DHE\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_IDEA\_128\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_SEED\_SHA  
 TLS1\_RSA\_WITH\_SEED\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_DES\_192\_CBC3\_SHA  
 TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_RSA\_DES\_192\_CBC3\_SHA  
 TLS1\_DHE\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_WITH\_AES\_128\_SHA  
 TLS1\_RSA\_IDEA\_128\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS1\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  
 TLS1\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS1\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
 TLS\_1\_2\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (custom override [Weak > Medium])  
 TLS\_1\_2\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (custom override [Weak > Medium])  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_1\_2\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS\_1\_2\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_1\_2\_RSA\_WITH\_AES\_128\_CBC\_SHA

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Check for Telnet Server Severity: 0

3306/tcp

Summary

A telnet Server is running at this host.  
  
 Experts in computer security, such as SANS Institute, and the members of the  
 comp.os.linux.security newsgroup recommend that the use of Telnet for remote  
 logins should be discontinued under all normal circumstances, for the following  
 reasons:  
  
 \* Telnet, by default, does not encrypt any data sent over the connection  
 (including passwords), and so it is often practical to eavesdrop on the  
 communications and use the password later for malicious purposes  
 anybody who  
 has access to a router, switch, hub or gateway located on the network between  
 the two hosts where Telnet is being used can intercept the packets passing by  
 and obtain login and password information (and whatever else is typed) with any  
 of several common utilities like tcpdump and Wireshark.  
  
 \* Most implementations of Telnet have no authentication that would ensure  
 communication is carried out between the two desired hosts and not intercepted  
 in the middle.  
  
 \* Commonly used Telnet daemons have several vulnerabilities discovered over  
 the years.

Description

A telnet server seems to be running on this port

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## MySQL/MariaDB Detection Severity: 0

3306/tcp

Summary

Detection of installed version of  
 MySQL/MariaDB.  
  
 Detect a running MySQL/MariaDB by getting the banner, Extract the version  
 from the banner and store the information in KB

Description

Scanner received a ER\_HOST\_NOT\_PRIVILEGED error from the remote MySQL/MariaDB server.  
Some tests may fail. Allow the scanner to access the remote MySQL server for better results.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N

## Detect Server type and version via Telnet Severity: 0

3306/tcp

Summary

This detects the Telnet Server's type and version by connecting to the server  
and processing the buffer received.  
This information gives potential attackers additional information about the  
system they are attacking. Versions and Types should be omitted  
where possible.

Description

Remote telnet banner :  
BHost 'Last-Pc' is not allowed to connect to this MariaDB server

Solution

Change the login banner to something generic.

CVSS (Base Score)

0.0 AV:N/AC:L/Au:N/C:N/I:N/A:N