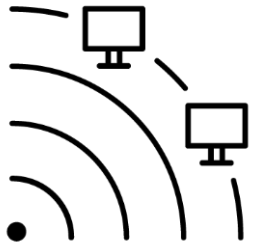


F-Secure Radar

Security Assessment Report

Company PL - demo-linux (10.50.2.161)

Report details

Scan finished: 04-01-2017

Generated by: User

Table of Contents

Press F9 to update

About this document

This security report has been generated by the F-Secure Radar vulnerability management solution and contains results of a security assessment analysing demo-linux (10.50.2.161). All information related to the assessment, as well as the identified security issues and vulnerabilities are documented in this report, together with concrete remediation advice. Individuals with permission from Company PL are authorized to view this document. This document contains confidential information.

About information security assessments

The goal of an information security assessment is to determine the level of security for an agreed component at any given time. Even though an assessment can at best give an excellent insight into the level of security for the given target, it should never be used as the sole process for ensuring information security.

An assessment can give an insight, which would otherwise be missed, but it cannot necessarily find all possible weaknesses and vulnerabilities, which would have been visible during analysis and design phases. That is, an assessment can reveal security problems, but it cannot prove the absence of them.

In addition, the defence and attack techniques evolve constantly. Sometimes a completely new class of vulnerabilities is discovered, which was simply not known before. For this reason, the results of an assessment expire as time passes, and it is recommended to regularly assess critical business functions.

1. Executive summary

1.1. Assessment background

The purpose of this assessment was to analyse the security of demo-linux (10.50.2.161). Additionally, it was checked whether programming or configuration mistakes existed, permitting attackers or malicious users to perform actions they otherwise wouldn't be able to perform.

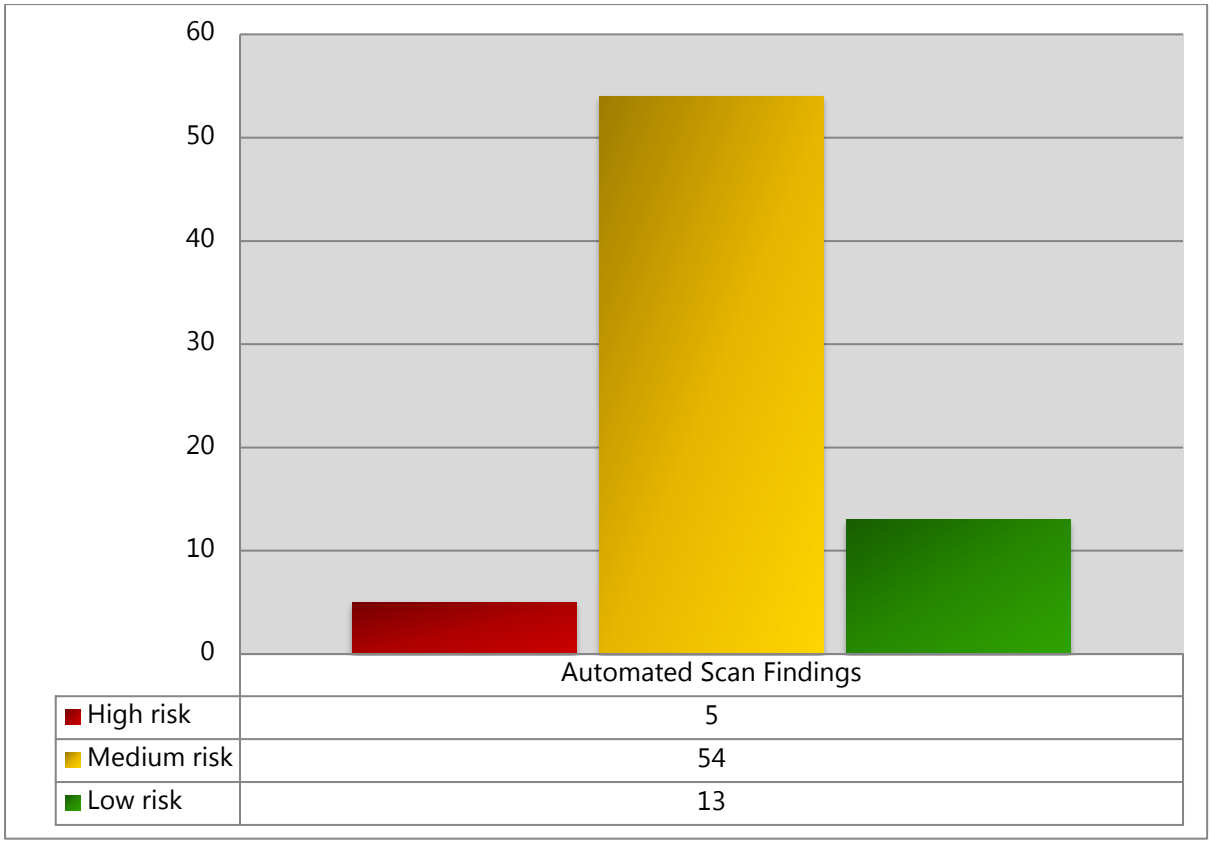
1.2. Conclusions

Based on vulnerabilities found, the overall security level is: **Low**

1.3. Vulnerability statistics

All vulnerabilities found throughout the security assessment are given a severity ranking, calculated using CVSSv2 metrics.

The illustration below allows managers to easily identify which areas that requires focus and shows if any immediate actions are required.



Informational findings: 12

2. Findings – demo-linux (10.50.2.161)

Platform and services identified:

Target	Description
Name	demo-linux (10.50.2.161)
Platform	Linux (Ubuntu)
Service	Name: www Port: TCP/443 Banner: HTTP/1.1 200 OK Date: Wed, 04 Jan 2017 09:12:07 GMT Server: Apache/2.2.16 (Ubuntu) Last-Modified: Tue, 16 Jul 2013 12:32:17 GMT ETag: "22e71-b1-4e1a02aec6c24" Accept-Ranges: bytes Content-Length: 177 Vary: Accept-Encoding Connection: close Content-Type: text/html

2.1. Automated scan results

2.1.1. High risk vulnerabilities

2.1.1.1 Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x DOS or buffer overflow

High AV: **Network** AC: **Low** Au: **None** C: **Complete** I: **Complete** A: **Complete** **10.0**

Vulnerability status: Unattended

Description

The remote web server is affected by an integer overflow vulnerability.

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the (1) allocator_alloc or (2) apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the (3) apr_rmm_malloc, (4) apr_rmm_calloc, or (5) apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows.

NOTE: some of these details are obtained from third party information. Versions prior to 2.2.17 have been reported as vulnerable.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to Apache web server version 2.2.17 or newer.

Tags

Apache, Version Based, Web Server

External references

CVE-2009-2412

http://www.securityfocus.com/bid/35949

2.1.1.2 Apache HTTP Server Byterange Filter Denial of Service Vulnerability

High AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Complete** **7.8**

Vulnerability status: Unattended

Description

The remote web server is affected by a denial of service vulnerability.

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest Apache version or disable the HTTP 'range' header by configuring Apache with the following setting 'Header unset Range' on Apache 1.3 or 'RequestHeader unset Range' for Apache 2

Tags

Apache, Version Based, Web Server

External references

CVE-2011-3192

http://www.securityfocus.com/bid/49303

2.1.1.3 End-of-life product: WordPress

High AV: **Network** AC: **High** Au: **None** C: **Complete** I: **Complete** A: **Complete** **7.6**

Vulnerability status: Unattended

Description

This version of the remote WordPress application has reached end-of-life status.

Active development for this version of WordPress has ended. New updates or patches will not be available.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Migrate to the latest WordPress version.

Tags

Version Based, Web application, Web Server, WordPress

2.1.1.4 Apache HTTP Server before 2.4.5 Unspecified Vulnerability

High AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **Partial** A: **Partial** **7.5**

Vulnerability status: Unattended

Description

The remote web server is affected by an unspecified vulnerability.

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in version 2.4.5.

Tags

Apache, Version Based, Web Server

External references

CVE-2013-2249

2.1.1.5 phpMyAdmin before 3.3.10.2 and 3.4.3.1 Multiple Vulnerabilities

High AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **Partial** A: **Partial** **7.5**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by multiple vulnerabilities.

[CVE-2011-2505] libraries/auth/swekey/swekey.auth.lib.php in the Swekey authentication feature in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 assigns values to arbitrary parameters referenced in the query string, which allows remote attackers to modify the SESSION superglobal array via a crafted request, related to a 'remote variable manipulation vulnerability'.

[CVE-2011-2506] setup/lib/ConfigGenerator.class.php in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 does not properly restrict the presence of comment closing delimiters, which allows remote attackers to conduct static code injection attacks by leveraging the ability to modify the SESSION superglobal array.

[CVE-2011-2507] libraries/server_synchronize.lib.php in the Synchronize implementation in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 does not properly quote regular expressions, which allows remote authenticated users to inject a PCRE e (aka PREG_REPLACE_EVAL) modifier, and consequently execute arbitrary PHP code, by leveraging the ability to modify the SESSION superglobal array.

[CVE-2011-2508] Directory traversal vulnerability in libraries/display_tbl.lib.php in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1, when a certain MIME transformation feature is enabled, allows remote authenticated users to include and execute arbitrary local files via a .. (dot dot) in a GLOBALS[mime_map][$meta->name][transformation] parameter.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-2505

CVE-2011-2506

CVE-2011-2507

CVE-2011-2508

http://www.securityfocus.com/archive/1/archive/1/518804/100/0/threaded

2.1.2. Medium risk vulnerabilities

2.1.2.1 Apache HTTP Server LD_LIBRARY PATH Privileges Escalation Vulnerability

Medium AV: **Local** AC: **Medium** Au: **None** C: **Complete** I: **Complete** A: **Complete** **6.9**

Vulnerability status: Unattended

Description

The remote web server is affected by a privileges escalation vulnerability.

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade Apache HTTP Server to version 2.4.2 or to the latest stable version.

Tags

Apache, Version Based, Web Server

External references

CVE-2012-0883

2.1.2.2 OpenSSL CCS Injection Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **Partial** A: **Partial** **6.8**

Vulnerability status: Unattended

Description

The remote OpenSSL is affected by the ChangeCipherSpec injection vulnerability.

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Vulnerability confirmed by an active check.
```

Recommendations

Upgrade OpenSSL to the latest stable version.

External references

CVE-2014-0224

CVE-2014-0224

http://www.securityfocus.com/bid/67899

http://www.securityfocus.com/archive/1/archive/1/534161/100/0/threaded

http://www.securityfocus.com/archive/1/archive/1/535181/100/0/threaded

2.1.2.3 WordPress before 3.9.2 Multiple Vulnerabilities

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **Partial** A: **Partial** **6.8**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by multiple vulnerabilities.

[CVE-2014-5205] wp-includes/pluggable.php in WordPress before 3.9.2 does not use delimiters during concatenation of action values and uid values in CSRF tokens, which makes it easier for remote attackers to bypass a CSRF protection mechanism via a brute-force attack.

[CVE-2014-5204] wp-includes/pluggable.php in WordPress before 3.9.2 rejects invalid CSRF nonces with a different timing depending on which characters in the nonce are incorrect, which makes it easier for remote attackers to bypass a CSRF protection mechanism via a brute-force attack.

[CVE-2014-5266] The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, does not limit the number of elements in an XML document, which allows remote attackers to cause a denial of service (CPU consumption) via a large document, a different vulnerability than CVE-2014-5265.

[CVE-2014-5265] The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, permits entity declarations without considering recursion during entity expansion, which allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.

[CVE-2014-5240] Cross-site scripting (XSS) vulnerability in wp-includes/pluggable.php in WordPress before 3.9.2, when Multisite is enabled, allows remote authenticated administrators to inject arbitrary web script or HTML, and obtain Super Admin privileges, via a crafted avatar URL.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 3.9.2.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-5204

CVE-2014-5205

CVE-2014-5240

CVE-2014-5265

CVE-2014-5266

http://www.securityfocus.com/bid/69096

http://www.securityfocus.com/bid/69096

http://www.securityfocus.com/bid/69096

http://www.securityfocus.com/bid/69146

http://www.securityfocus.com/bid/69146

2.1.2.4 WordPress before 4.5 Multiple Vulnerabilities

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **Partial** A: **Partial** **6.8**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by multiple vulnerabilities.

[CVE-2016-4029] WordPress before 4.5 does not consider octal and hexadecimal IP address formats when determining an intranet address, which allows remote attackers to bypass an intended SSRF protection mechanism via a crafted address.

[CVE-2016-6634] Cross-site scripting (XSS) vulnerability in the network settings page in WordPress before 4.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

[CVE-2016-6635] Cross-site request forgery (CSRF) vulnerability in the wp_ajax_wp_compression_test function in wp-admin/includes/ajax-actions.php in WordPress before 4.5 allows remote attackers to hijack the authentication of administrators for requests that change the script compression option.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.5.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2016-4029

CVE-2016-6634

CVE-2016-6635

2.1.2.5 WordPress Unauthorized Access to Account Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **Partial** A: **Partial** **6.8**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a cryptographic issues.

WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 might allow remote attackers to obtain access to an account idle since 2008 by leveraging an improper PHP dynamic type comparison for an MD5 hash.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9037

http://www.securityfocus.com/bid/71238

2.1.2.6 phpMyAdmin Bookmarks Handling SQL Query Injection Vulnerability

Medium AV: **Network** AC: **Low** Au: **Single Instance** C: **Partial** I: **Partial** A: **Partial** **6.5**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by an sql injection vulnerability.

The PMA_Bookmark_get function in libraries/bookmark.lib.php in phpMyAdmin 2.11.x before 2.11.11.3, and 3.3.x before 3.3.9.2, does not properly restrict bookmark queries, which makes it easier for remote authenticated users to trigger another user's execution of a SQL query by creating a bookmark.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-0987

2.1.2.7 WordPress before 4.6.1 Path Traversal Vulnerability

Medium AV: **Network** AC: **Low** Au: **Single Instance** C: **Partial** I: **Partial** A: **Partial** **6.5**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a path traversal vulnerability.

Directory traversal vulnerability in the File_Upload_Upgrader class in wp-admin/includes/class-file-upload-upgrader.php in the upgrade package uploader in WordPress before 4.6.1 allows remote authenticated users to access arbitrary files via a crafted urlholder parameter.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.6.1.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2016-7169

2.1.2.8 phpMyAdmin 'libraries/auth/swekey/swekey.auth.lib.php' Sensitive Data Access Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **Partial** A: **Partial** **6.4**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by a sensitive data access vulnerability.

libraries/auth/swekey/swekey.auth.lib.php in phpMyAdmin 3.x before 3.3.10.3 and 3.4.x before 3.4.3.2 does not properly manage sessions associated with Swekey authentication, which allows remote attackers to modify the SESSION superglobal array, other superglobal arrays, and certain swekey.auth.lib.php local variables via a crafted query string.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-2719

http://www.securityfocus.com/bid/48874

http://www.securityfocus.com/archive/1/archive/1/518967/100/0/threaded

http://www.securityfocus.com/archive/1/archive/1/519155/100/0/threaded

2.1.2.9 WordPress Server-Side Request Forgery Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **Partial** A: **None** **6.4**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a server-side request forgery vulnerability.

wp-includes/http.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to conduct server-side request forgery (SSRF) attacks by referring to a 127.0.0.0/8 resource.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9038

http://www.securityfocus.com/bid/71234

2.1.2.10 Apache HTTP Server before 2.4.25 Response Handler Split Privilege Escalation Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **Partial** **5.8**

Vulnerability status: Unattended

Description

The remote web server is affected by a privilege escalation vulnerability.

Apache HTTP Server before 2.4.25 is affected by a privilege escalation vulnerability. The server does not strictly parse HTTP header data. A remote user can submit a specially crafted URL to cause the target server to return a split response. A remote user can exploit this to spoof content on the target server, attempt to poison any intermediate web caches, or conduct cross-site scripting attacks.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in version 2.4.25.

Tags

Apache, Version Based, Web Server

External references

CVE-2016-8743

2.1.2.11 WordPress before 4.2.1 Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **Partial** A: **None** **5.8**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a cross-site scripting vulnerability.

Stored XSS vulnerability in WordPress before 4.2.1 could allow unauthenticated attacker to inject JavaScript in WordPress comments and execute arbitrary code on the server via the plugin and theme editors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the WordPress module. The vendor has prepared a fix for this issue in version 4.2.1.

Tags

Version Based, Web application, Web Server, WordPress

2.1.2.12 Apache HTTP Server 2.2.x before 2.2.25 Code Execution Vulnerability

Medium AV: **Network** AC: **High** Au: **None** C: **Partial** I: **Partial** A: **Partial** **5.1**

Vulnerability status: Unattended

Description

The remote web server is affected by a code execution vulnerability.

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in version 2.2.25.

Tags

Apache, Version Based, Web Server

External references

CVE-2013-1862

http://www.securityfocus.com/bid/64758

2.1.2.13 Apache APR-util 'apr_brigade_split_line()' Denial of Service Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote web server is affected by a denial of service vulnerability.

The apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest Apache version.

Tags

Apache, Version Based, Web Server

External references

CVE-2010-1623

http://www.securityfocus.com/bid/43673

2.1.2.14 Apache HTTP Server before 2.4.8 Denial of Service Vulnerabilities

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote web server is affected by denial of service vulnerabilities.

[CVE-2013-6438] The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

[CVE-2014-0098] The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in version 2.4.8.

Tags

Apache, Version Based, Web Server

External references

CVE-2013-6438

CVE-2014-0098

http://www.securityfocus.com/bid/66303

http://www.securityfocus.com/archive/1/archive/1/534161/100/0/threaded

2.1.2.15 Apache HTTP Server CVE-2014-0231 Remote Denial of Service Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote web server is affected by denial of service vulnerability.

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in versions 2.2.29 and 2.4.10.

Tags

Apache, Version Based, Web Server

External references

CVE-2014-0231

http://www.securityfocus.com/bid/68742

http://www.securityfocus.com/archive/1/archive/1/535181/100/0/threaded

2.1.2.16 Apache HTTP Server mod_proxy Module Input Validation Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **None** A: **None** **5.0**

Vulnerability status: Unattended

Description

The remote web server is affected by an input validation vulnerability.

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest Apache version.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-3368

http://www.securityfocus.com/bid/49957

http://www.securityfocus.com/archive/1/archive/1/535181/100/0/threaded

2.1.2.17 Apache: Expat XML Parsing Remote Denial of Service Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote web server is affected by a denial of service vulnerability.

The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with malformed UTF-8 sequences that trigger a buffer over-read, related to the doProlog function in lib/xmlparse.c, a different vulnerability than CVE-2009-2625 and CVE-2009-3720. Apache2 versions prior to 2.2.17 bundle this library and have been reported vulnerable.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest Apache version.

Tags

Apache, Version Based, Web Server

External references

CVE-2009-3560

http://www.securityfocus.com/bid/37203

2.1.2.18 Directory listings enabled

Medium AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **None** A: **None** **5.0**

Vulnerability status: Unattended

Description

Directory listings enable an attacker to learn details about the framework in use.

Directory listings enable an attacker to learn details about the framework in use, like exact version number and information about installed components.

An attacker can gain information about the web application by browsing directory listings that reveal files and folder hierarchy in the application. This information can be used to exploit vulnerabilities in the web application.

Any sensitive resources within your web root should be properly access-controlled and should not be accessible to an unauthorized party who knows the URL. Nevertheless, directory listings can aid an attacker by enabling them to quickly identify the resources at a given path, and proceed directly to analyzing and attacking them.

The vulnerability is based on the following retrieved information from 443/TCP:

```
https://10.50.2.161:443/icons/small/
```

Recommendations

There is not usually any good reason to provide directory listings, and disabling them may place additional hurdles in the path of an attacker. This can normally be achieved in two ways:

- Configure your web server to prevent directory listings for all paths beneath the web root;

- Place into each directory a default file (such as index.htm) which the web server will display instead of returning a directory listing.

Tags

Web Server

2.1.2.19 Git repository exposed

Medium AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **None** A: **None** **5.0**

Vulnerability status: Unattended

Description

The remote web server discloses internal files of Git repository.

Git repository on the remote server is served by web server. This can be used to download source code and potentially private information.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Found exposed git repository at '/.git/config'. Content:
[core]
repositoryformatversion = 0
filemode = true
bare = false
logallrefupdates = true
```

Recommendations

Disable access to .git directory.

2.1.2.20 phpMyAdmin Installationion Path Disclosure Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **None** A: **None** **5.0**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by an information disclosure vulnerability.

phpMyAdmin 2.11.x before 2.11.11.2, and 3.3.x before 3.3.9.1, does not properly handle the absence of the (1) README, (2) ChangeLog, and (3) LICENSE files, which allows remote attackers to obtain the installation path via a direct request for a nonexistent file.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-0986

2.1.2.21 SSL certificate is not valid

Medium AV: **Network** AC: **Low** Au: **None** C: **Partial** I: **None** A: **None** **5.0**

Vulnerability status: Unattended

Description

The remote SSL server's certificate is invalid.

The remote SSL server's certificate is invalid. It was not possible to confirm validity of the Certificate. Most probably, the certificate has been 'self-signed'.

This is especially dangerous because users of the website cannot validate if the remote server is the correct one, or if an attacker attempts to conduct a man-in-the-middle attack. Moreover, browsers will usually return an 'invalid certificate'-error upon visit of the website. If users are taught to accept such warnings it can have big consequences later on if users fall victim to a man-in-the-middle attack.

The vulnerability is based on the following retrieved information from 443/TCP:

```
The certificate is NOT valid. It is issued by CN=localhost. Verification status:
UntrustedRoot. Information: A certificate chain processed, but terminated in a
root certificate which is not trusted by the trust provider.


Certificate's CN: localhost
```

Recommendations

Generate a new valid SSL certificate.

Tags

SSL, TLS

2.1.2.22 WordPress before 4.5.3 Denial of Service Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a denial of service vulnerability.

The oEmbed protocol implementation in WordPress before 4.5.3 allows remote attackers to cause a denial of service via unspecified vectors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.5.3.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2016-5836

2.1.2.23 WordPress before 4.5.3 Multiple Vulnerabilities

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **Partial** A: **None** **5.0**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by multiple vulnerabilities.

[CVE-2016-5832] The customizer in WordPress before 4.5.3 allows remote attackers to bypass intended redirection restrictions via unspecified vectors.

[CVE-2016-5833] Cross-site scripting (XSS) vulnerability in the column_title function in wp-admin/includes/class-wp-media-list-table.php in WordPress before 4.5.3 allows remote attackers to inject arbitrary web script or HTML via a crafted attachment name, a different vulnerability than CVE-2016-5834.

[CVE-2016-5834] Cross-site scripting (XSS) vulnerability in the wp_get_attachment_link function in wp-includes/post-template.php in WordPress before 4.5.3 allows remote attackers to inject arbitrary web script or HTML via a crafted attachment name, a different vulnerability than CVE-2016-5833.

[CVE-2016-5835] WordPress before 4.5.3 allows remote attackers to obtain sensitive revision-history information by leveraging the ability to read a post, related to wp-admin/includes/ajax-actions.php and wp-admin/revision.php.

[CVE-2016-5837] WordPress before 4.5.3 allows remote attackers to bypass intended access restrictions and remove a category attribute from a post via unspecified vectors.

[CVE-2016-5838] WordPress before 4.5.3 allows remote attackers to bypass intended password-change restrictions by leveraging knowledge of a cookie.

[CVE-2016-5839] WordPress before 4.5.3 allows remote attackers to bypass the sanitize_file_name protection mechanism via unspecified vectors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.5.3.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2016-5832

CVE-2016-5833

CVE-2016-5834

CVE-2016-5835

CVE-2016-5837

CVE-2016-5838

CVE-2016-5839

2.1.2.24 WordPress 'class-phpass' Denial of Service Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a denial of service vulnerability.

wp-includes/class-phpass.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to cause a denial of service (CPU consumption) via a long password that is improperly handled during hashing, a similar issue to CVE-2014-9016.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9034

http://www.securityfocus.com/bid/71233

2.1.2.25 Apache HTTP Server Scoreboard Local Security Bypass Vulnerability

Medium AV: **Local** AC: **Low** Au: **None** C: **Partial** I: **Partial** A: **Partial** **4.6**

Vulnerability status: Unattended

Description

The remote web server is affected by a local security-bypass vulnerability.

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version (2.2.22 or newer).

Tags

Apache, Version Based, Web Server

External references

CVE-2012-0031

http://www.securityfocus.com/bid/51407

2.1.2.26 Apache HTTP Server Bad Request Error Documents Information Disclosure Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by an information disclosure vulnerability.

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version.

Tags

Apache, Version Based, Web Server

External references

CVE-2012-0053

http://www.securityfocus.com/bid/51706

http://www.securityfocus.com/archive/1/archive/1/535181/100/0/threaded

2.1.2.27 Apache HTTP Server before 2.2.24-dev and 2.4.4 Cross-Site Scripting Vulnerabilities

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by cross-site scripting vulnerabilities.

[CVE-2012-3499] Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

[CVE-2012-4558] Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in versions 2.2.24 and 2.4.4

Tags

Apache, Version Based, Web Server

External references

CVE-2012-3499

CVE-2012-4558

http://www.securityfocus.com/bid/64758

2.1.2.28 Apache HTTP Server before 2.2.25 DAV Denial of Service Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **None** A: **Partial** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by a denial of service vulnerability.

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version. The vendor has prepared a fix for this issue in version 2.2.25.

Tags

Apache, Version Based, Web Server

External references

CVE-2013-1896

2.1.2.29 Apache HTTP Server mod_proxy_balancer DoS Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **None** A: **Partial** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by a denial of service vulnerability.

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary 'error state' in the backend server) via a malformed HTTP request.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest Apache version.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-3348

http://www.securityfocus.com/bid/49616

2.1.2.30 phpMyAdmin before 3.3.10.1 and 3.4.1 Multiple Cross-Site Scripting Vulnerabilities

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by a cross-site scripting vulnerability.

Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.3.x before 3.3.10.1 and 3.4.x before 3.4.1 allow remote attackers to inject arbitrary web script or HTML via a crafted table name that triggers improper HTML rendering on a Tracking page, related to (1) libraries/tbl_links.inc.php and (2) tbl_tracking.php.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the 3.3.10.1 or 3.4.1 (or latest) version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-1940

2.1.2.31 phpMyAdmin Database Search Script Arbitrary HTML Code Insertion Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by an arbitrary HTML code insertion vulnerability.

Cross-site scripting (XSS) vulnerability in the PMA_linkOrButton function in libraries/common.lib.php in the database (db) search script in phpMyAdmin 2.11.x before 2.11.11.1 and 3.x before 3.3.8.1 allows remote attackers to inject arbitrary web script or HTML via a crafted request.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2010-4329

http://www.securityfocus.com/bid/45100

2.1.2.32 phpMyAdmin 'simplexml_load_string()' Function Information Disclosure Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by an information disclosure vulnerability.

The simplexml_load_string function in the XML import plug-in (libraries/import/xml.php) in phpMyAdmin 3.4.x before 3.4.7.1 and 3.3.x before 3.3.10.5 allows remote authenticated users to read arbitrary files via XML data containing external entity references, aka an XML external entity (XXE) injection attack.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to phpMyAdmin 3.4.7.1 or newer (or 3.3.10.5) or apply the related patches.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-4107

http://www.securityfocus.com/bid/50497

2.1.2.33 Remote server supports SSL 3.0

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server uses an old version of SSL.

The remote service accepts connections encrypted using SSL 3.0 which is obsolete and lacks key features. It is safe to disable it, because all modern clients support newer versions.

The vulnerability is based on the following retrieved information from 443/TCP:

```
The remote host supports connections using SSL 3.0 protocol.
```

Recommendations

Disable SSL 3.0 support and use TLS 1.2 instead or TLS 1.1 where 1.2 is not available.

Tags

SSL

2.1.2.34 Remote server supports TLS 1.0

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server uses an old version of TLS.

The remote service accepts connections encrypted using TLS 1.0 which is obsolete and lacks key features. It is safe to disable it, because all modern clients support newer versions.

The vulnerability is based on the following retrieved information from 443/TCP:

```
The remote host supports connections using TLS 1.0 protocol.
```

Recommendations

Disable TLS 1.0 support and use TLS 1.2 instead or TLS 1.1 where 1.2 is not available.

Tags

TLS

2.1.2.35 SSL/TLS RC4 Cipher Suites Supported

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote service supports the RC4 cipher suites.

[CVE-2013-2566] The RC4 algorithm, as used in the TLS protocol and SSL protocol, 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.

[CVE-2015-2808] The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the 'Bar Mitzvah' issue.

The vulnerability is based on the following retrieved information from 443/TCP:

```
RC4 cipher suites supported.
```

Recommendations

Disable RC4 cipher suites in the service's configuration. Migration to TLS1.2 and AES-GCM cipher suites is highly recommended.

Tags

SSL, TLS

External references

CVE-2013-2566

CVE-2015-2808

http://www.securityfocus.com/bid/58796

http://www.securityfocus.com/bid/73684

2.1.2.36 SSL3 POODLE vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote server is vulnerable to a man-in-the-middle attack.

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses non-deterministic CBC padding, which makes it easier for man-in-the-middle attackers to decrypt data via a padding-oracle attack, aka the 'POODLE' issue.

POODLE allows an attacker who can control the Internet connection between your browser and server to e.g. hijack session cookies or potentially execute scripts on your behalf.

The vulnerability is based on the following retrieved information from 443/TCP:

```
SSL3 is enabled and TLS_FALLBACK_SCSV is not supported by the server.
```

Recommendations

The recommended solution is to disable SSL3 support. If this is impossible due to backward compatibility reasons the TLS_FALLBACK_SCSV cipher suite should be enabled.

Tags

SSL

External references

CVE-2014-3566

http://www.securityfocus.com/bid/70574

2.1.2.37 WordPress 2.x and 3.x Stored Cross Site Scripting

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a cross-site scripting vulnerability.

A security flaw in WordPress 3 allows injection of JavaScript into certain text fields. In particular, the problem affects comment boxes on WordPress posts and pages. By default they do not authentication.

The JavaScript injected into a comment is executed when the target user views it, either on a blog post, a page, or in the Comments section of the administrative Dashboard. The attacker can leave a comment containing the JavaScript and some links in order to put the comment in the moderation queue. The exploit is not then visible to normal users, search engines, etc.

When a blog administrator goes to the Dashboard/Comments section to review new comments, the JavaScript gets executed. The script can then perform operations with administrator privileges, such as changing the current user's password, adding a new administrator account. These operations happen in the background without the user seeing anything out of ordinary.

The attacker can also write new PHP code on the server via the plugin editor, and another AJAX request can be used to execute it instantaneously, whereby the attacker gains operating system level access on the server.

[CVE-2014-9031] Cross-site scripting (XSS) vulnerability in the wptexturize function in WordPress before 3.7.5, 3.8.x before 3.8.5, and 3.9.x before 3.9.3 allows remote attackers to inject arbitrary web script or HTML via crafted use of shortcode brackets in a text field, as demonstrated by a comment or a post.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of Wordpress. The vendor has prepared a fix for this issue in version 4.0.1. Wordpress 4.0 uses a different kind of regular expression and is NOT vulnerable to this problem.

Workarounds:

The problem occurs in a text formatting function called wptexturize() which is normally executed for each comment and other blocks of text. The function replaces certain simple characters with fancier HTML entities. Texturizing can be easily disabled by adding a return statement in the beginning of the function in wp-includes/formatting.php:

function wptexturize($text) {

return $text; // ADD THIS LINE

global $wp_cockneyreplace;

This changes how some punctuation marks look like but the difference is quite minor.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9031

http://www.securityfocus.com/bid/71237

2.1.2.38 Wordpress before 4.1.2 Cross Site-Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a cross-site scripting vulnerability.

Not clear desription of add_query_arg() and remove_query_arg() functions caused using them in an insecure way. This could allow many plugins to be vulnerable to cross-site scripting.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.1.2.

Tags

Version Based, Web application, Web Server, WordPress

2.1.2.39 WordPress before 4.1.2 Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a cross-site scripting vulnerability.

Multiple cross-site scripting (XSS) vulnerabilities in WordPress before 4.1.2, when MySQL is used without strict mode, allow remote attackers to inject arbitrary web script or HTML via a (1) four-byte UTF-8 character or (2) invalid character that reaches the database layer.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.1.2.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2015-3438

2.1.2.40 WordPress before 4.2.1 Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a cross-site scripting vulnerability.

Cross-site scripting (XSS) vulnerability in wp-includes/wp-db.php in WordPress before 4.2.1 allows remote attackers to inject arbitrary web script or HTML via a long comment that is improperly stored because of limitations on the MySQL TEXT data type.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.2.1.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2015-3440

2.1.2.41 WordPress before 4.3.1 Multiple Vulnerabilities

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by multiple vulnerabilities.

[CVE-2015-5714] Cross-site scripting (XSS) vulnerability in WordPress before 4.3.1 allows remote attackers to inject arbitrary web script or HTML by leveraging the mishandling of unclosed HTML elements during processing of shortcode tags.

[CVE-2015-7989] Cross-site scripting (XSS) vulnerability in the user list table in WordPress before 4.3.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted e-mail address, a different vulnerability than CVE-2015-5714.

[CVE-2015-5715] The mw_editPost function in wp-includes/class-wp-xmlrpc-server.php in the XMLRPC subsystem in WordPress before 4.3.1 allows remote authenticated users to bypass intended access restrictions, and arrange for a private post to be published and sticky, via unspecified vectors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.3.1.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2015-5714

CVE-2015-5715

CVE-2015-7989

http://www.securityfocus.com/bid/76744

http://www.securityfocus.com/bid/76745

http://www.securityfocus.com/bid/76748

2.1.2.42 WordPress before 4.4.1 Authenticated Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a cross-site scripting vulnerability.

Multiple cross-site scripting (XSS) vulnerabilities in wp-includes/class-wp-theme.php in WordPress before 4.4.1 allow remote attackers to inject arbitrary web script or HTML via a (1) stylesheet name or (2) template name to wp-admin/customize.php.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.4.1.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2016-1564

2.1.2.43 WordPress before 4.6.1 Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by a cross-site scripting vulnerability.

Cross-site scripting (XSS) vulnerability in the media_handle_upload function in wp-admin/includes/media.php in WordPress before 4.6.1 might allow remote attackers to inject arbitrary web script or HTML by tricking an administrator into uploading an image file that has a crafted filename.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.6.1.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2016-7168

http://www.securityfocus.com/bid/92841

2.1.2.44 WordPress CSS Token Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a cross-site scripting vulnerability.

Cross-site scripting (XSS) vulnerability in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via a crafted Cascading Style Sheets (CSS) token sequence in a post.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9036

http://www.securityfocus.com/bid/71236

2.1.2.45 WordPress Password Reset Email Security Bypass Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **Partial** I: **None** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a security bypass vulnerability.

wp-login.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 might allow remote attackers to reset passwords by leveraging access to an e-mail account that received a password-reset message.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9039

http://www.securityfocus.com/bid/71231

2.1.2.46 WordPress Press This Cross-Site Scripting Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote Wordpress application is affected by a cross-site scripting vulnerability.

Cross-site scripting (XSS) vulnerability in Press This in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2014-9035

http://www.securityfocus.com/bid/71236

2.1.2.47 SSL certificate uses SHA1 signature

Medium AV: **Network** AC: **Low** Au: **Single Instance** C: **Partial** I: **None** A: **None** **4.0**

Vulnerability status: Unattended

Description

The remote server's SSL certificate uses SHA1 signature.

SHA1 is widely used in SSL certificates but has been deprecated since 2011. There are known attacks for the SHA1 hash function so it cannot be considered safe for PKI. Microsoft Windows and Google Chrome will stop accepting SHA1 certificates by 2017.

The vulnerability is based on the following retrieved information from 443/TCP:

```
The SSL certificate uses SHA1 signature and expires in or after 2017. Google
Chrome (V40) does not show a "green lock" to indicate that the connection is
secure. Google Chrome (V41 or later) will treat the connection to this server as
"affirmatively insecure". Subresources loaded from such domain will be treated as
"active mixed content".

Certificate's CN: localhost
```

Recommendations

Renew the certificate as soon as possible and ensure it is signed with SHA2.

Tags

SSL, TLS

2.1.2.48 WordPress before 4.2.3 Multiple Vulnerabilities

Medium AV: **Network** AC: **Low** Au: **Single Instance** C: **None** I: **Partial** A: **None** **4.0**

Vulnerability status: Unattended

Description

The remote WordPress application is affected by multiple vulnerabilities.

[CVE-2015-5622] Cross-site scripting (XSS) vulnerability in WordPress before 4.2.3 allows remote authenticated users to inject arbitrary web script or HTML by leveraging the Author or Contributor role to place a crafted shortcode inside an HTML element, related to wp-includes/kses.php and wp-includes/shortcodes.php.

[CVE-2015-5623] WordPress before 4.2.3 does not properly verify the edit_posts capability, which allows remote authenticated users to bypass intended access restrictions and create drafts by leveraging the Subscriber role, as demonstrated by a post-quickdraft-save action to wp-admin/post.php.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected WordPress version: 3.5.2 at https://10.50.2.161:443/wordpress/
```

Recommendations

Upgrade to the latest version of the Wordpress module. The vendor has prepared a fix for this issue in version 4.2.3.

Tags

Version Based, Web application, Web Server, WordPress

External references

CVE-2015-5622

CVE-2015-5623

2.1.3. Low risk vulnerabilities

2.1.3.1 phpMyAdmin before 4.17 XSS Vulnerability

Low AV: **Network** AC: **Medium** Au: **Single Instance** C: **None** I: **Partial** A: **None** **3.5**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by a cross-site scripting vulnerability.

Cross-site scripting (XSS) vulnerability in import.php in phpMyAdmin before 4.1.7 allows remote authenticated users to inject arbitrary web script or HTML via a crafted filename in an import action.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the phpMyAdmin. First fixed in 4.1.7.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2014-1879

http://www.securityfocus.com/bid/65717

2.1.3.2 SSL supports medium strength ciphers (128 bit)

Low AV: **Network** AC: **Medium** Au: **Single Instance** C: **Partial** I: **None** A: **None** **3.5**

Vulnerability status: Unattended

Description

The remote web server uses 128 bit encryption.

The remote host offers medium strength encryption cipher (128 bit), which is the lowest minimum, according to best security practices. For more information about SSL ciphers see: http://www.openssl.org/docs/apps/ciphers.html#CIPHER_STRINGS

The vulnerability is based on the following retrieved information from 443/TCP:

```
The remote host supports connections using medium strength cipher suites:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
```

Recommendations

If possible, disable support for 128 bit encryption to ensure only high strength ciphers are used to establish secure connections.

Tags

SSL, TLS

External references

CVE-2016-2183

https://sweet32.info/

2.1.3.3 CN in the certificate does not match actual host name (FQDN)

Low AV: **Adjacent Network** AC: **High** Au: **None** C: **Partial** I: **Partial** A: **None** **3.2**

Vulnerability status: Unattended

Description

Common Name in SSL Certificate of the remote host does not match actual FQDN.

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

The vulnerability is based on the following retrieved information from 443/TCP:

```
CN is a non-resolvable name (localhost) and does not match FQDN.
```

Recommendations

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.

Tags

SSL, TLS

2.1.3.4 Apache MultiViews Information Disclosure

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

The remote web server is affected by an information disclosure vulnerability.

It is possible to retrieve the file names served by the server that might not be meant for browsing.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Information retrieved from Alternates HTTP header field:
{"index.html" 1 {type text/html} {length 177}}
Path: /index
```

Recommendations

It is strongly recommended to disable MultiViews option in Apache configuration file.

Tags

Apache, Version Based

2.1.3.5 Cookie without httpOnly flag set

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

HTTP session cookies might be vulnerable to cross-site scripting attacks.

The remote web application uses cookies. One or more of those cookies are not set with the 'HttpOnly' attribute, meaning that a malicious client-side script such as JavaScript can read them.

'HttpOnly' is a security mechanism to protect against cross-site scripting attacks that was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers support it.

Note that:

- It is not possible to verify if the web application contains login functionality and use affected cookie for session management.

- 'HttpOnly' can be circumvented in some cases.

- The absence of this attribute does not mean that the web application is automatically vulnerable to cross-site scripting attacks.

- Some web applications need to manipulate the session cookie through client-side scripts and the 'HttpOnly' attribute cannot be set.

The vulnerability is based on the following retrieved information from 443/TCP:

```
PHPSESSID=o4p3pmk35uea57v1rumq4omo66; path=/
```

Recommendations

Apply 'HttpOnly' to the affected cookies.

Tags

Web Server

2.1.3.6 Missing HTTP security headers

Low AV: **Network** AC: **High** Au: **None** C: **None** I: **Partial** A: **None** **2.6**

Vulnerability status: Unattended

Description

The remote web server is missing optional HTTP security headers

The website's security posture can be enhanced by defining several HTTP headers designed for improving end user security. As today's attacks increasingly target the client, the use of security enhancing browser features is encouraged.

Strict-Transport-Security

HTTP Strict Transport Security header instructs the browser to access the site using only HTTPS connections. The header mitigates the effects of man-in-the-middle attacks against end users. Even though the header is not yet supported by all browser vendors, it is likely to be included in future versions of popular browsers.

X-Content-Type-Options: nosniff

Internet Explorer has historically had MIME-type detection features which enable an attacker to execute JavaScript from a plaintext file. The above header instructs the browser to strictly follow the MIME-type defined in the Content header, preventing XSS attacks in certain attack scenarios where user uploaded documents are served.

X-XSS-Protection 1; mode=block

Some modern browsers such as IE8 and Google Chrome contain an XSS filter which tries to prevent exploitation of reflected cross site scripting vulnerabilities. Websites can explicitly define the browser to block such attacks. The block mode instructs the browser to block the whole page instead of modifying the server response if an attack is detected.

X-Frame-Options: DENY

If a website allows its content to be presented within a third party frame, an attacker can perform so-called clickjacking attacks which are similar to Cross-Site Request Forgery. These attacks can be prevented with adding an X-Frame-Options header which instructs the browser not to render the website within a frame.

Content-Security-Policy

Is a declarative policy that lets the authors (or server administrators) of a web application inform the client about the sources from which the application expects to load resources. To mitigate XSS attacks, for example, a web application can declare that it only expects to load script from specific, trusted sources. This declaration allows the client to detect and block malicious scripts injected into the application by an attacker. Content Security Policy is not intended as a first line of defence against content injection vulnerabilities. Instead, CSP is best used as defence-in-depth, to reduce the harm caused by content injection attacks.

The vulnerability is based on the following retrieved information from 443/TCP:

```
The following HTTP headers are missing:
Strict-Transport-Security
X-Content-Type-Options
X-XSS-Protection
X-Frame-Options
Content-Security-Policy
```

Recommendations

Perform cost/benefit analysis for implementing the listed HTTP security headers.

Tags

Web Server

2.1.3.7 phpMyAdmin Print View Implementation Multiple Cross-Site Scripting Vulnerabilities

Low AV: **Network** AC: **High** Au: **None** C: **None** I: **Partial** A: **None** **2.6**

Vulnerability status: Unattended

Description

The remote PHPMyAdmin is affected by a cross-site scripting Vulnerabilities.

Multiple cross-site scripting (XSS) vulnerabilities in the table Print view implementation in tbl_printview.php in phpMyAdmin before 3.3.10.3 and 3.4.x before 3.4.3.2 allow remote authenticated users to inject arbitrary web script or HTML via a crafted table name.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Detected phpMyAdmin version: 3.3.7 at https://10.50.2.161:443/phpmyadmin/
```

Recommendations

Upgrade to the latest version of the PHPMyAdmin module.

Tags

phpMyAdmin, Version Based, Web application, Web Server

External references

CVE-2011-2642

http://www.securityfocus.com/bid/48874

2.1.3.8 SSL cookie without secure flag set

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

The web application cookies does not have the secure flag set

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain which issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

Note that:

- The vulnerability might be marked as a potential since it is not possible to confirm if the affected cookie(s) contain sensitive data such as the user's session token.

- It is not possible to verify if the web application contains login functionality and use affected cookie for session management.

- If only SSL connections are allowed towards the host e.g. if only TCP/443 is open the cookie will never be submitted over an unencrypted connection unless an active man-in-the-middle attack is performed towards the end-user.

The vulnerability is based on the following retrieved information from 443/TCP:

```
PHPSESSID=o4p3pmk35uea57v1rumq4omo66; path=/
```

Recommendations

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Tags

SSL, TLS

2.1.3.9 SSL Forward Secrecy is supported but not preferred

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

The remote SSL server does not enforce forward secrecy.

Forward secrecy (abbreviation: FS, also known as perfect forward secrecy or PFS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. An attacker, who obtained one of the keys, can use it to decrypt conversation (including previously captured traffic). Forward secrecy allows encrypted traffic to stay secret even if the private key is compromised in the future.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Server offers ephemeral ciphers, but there is no order of preference.
```

Recommendations

In SSL server configuration set ECDHE and/or DHE cipher suites as preferred.

Tags

SSL, TLS

2.1.3.10 TLS 1.2 is not supported

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

The remote SSL server does not support TLS 1.2.

TLS 1.2 is the newest version of Transport Layer Security Protocol and should be used as the main protocol with TLS 1.1 and 1.0 left only for backward compatibility. It introduces GCM and CCM modes of AES cipher.

The vulnerability is based on the following retrieved information from 443/TCP:

```
TLS 1.2 is not supported.
```

Recommendations

It is highly recommended to enable TLS 1.2 support in SSL server configuration if available. If your server does not support TLS 1.2 consider an upgrade.

Tags

TLS

2.1.3.11 TLS supports compression which may lead to information leakage (CRIME attack)

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

The remote TLS service is affected by an information leakage vulnerability.

The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.

The vulnerability is based on the following retrieved information from 443/TCP:

```
This service supports TLS compression.
```

Recommendations

Disable TLS compression support.

Tags

TLS

External references

CVE-2012-4929

http://www.securityfocus.com/bid/55704

2.1.3.12 Web Server TLS BREACH Attack

Low AV: **Network** AC: **High** Au: **None** C: **Partial** I: **None** A: **None** **2.6**

Vulnerability status: Unattended

Description

By observing the length of compressed HTTPS responses, an attacker may be able to derive plaintext secrets from the ciphertext of an HTTPS stream.

While CRIME was mitigated by disabling TLS/SPDY compression (and by modifying gzip to allow for explicit separation of compression contexts in SPDY), BREACH attacks HTTP responses. These are compressed using the common HTTP compression, which is much more common than TLS-level compression. This allows essentially the same attack demonstrated by Duong and Rizzo, but without relying on TLS-level compression (as they anticipated).

BREACH is a category of vulnerabilities and not a specific instance affecting a specific piece of software. To be vulnerable, a web application must:

- Be served from a server that uses HTTP-level compression

- Reflect user-input in HTTP response bodies

- Reflect a secret (such as a CSRF token) in HTTP response bodies

Additionally, while not strictly a requirement, the attack is helped greatly by responses that remain mostly the same (modulo the attacker's guess). This is because the difference in size of the responses measured by the attacker can be quite small. Any noise in the side-channel makes the attack more difficult (though not impossible).

It is important to note that the attack is agnostic to the version of TLS/SSL, and does not require TLS-layer compression. Additionally, the attack works against any cipher suite. Against a stream cipher, the attack is simpler; the difference in sizes across response bodies is much more granular in this case. If a block cipher is used, additional work must be done to align the output to the cipher text blocks.

The vulnerability is based on the following retrieved information from 443/TCP:

```
The remote server uses following compression types: gzip

HTTP/1.1 200 OK
Date: Wed, 04 Jan 2017 09:12:28 GMT
Server: Apache/2.2.16 (Ubuntu)
Last-Modified: Tue, 16 Jul 2013 12:32:17 GMT
ETag: "22e71-b1-4e1a02aec6c24"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 146
Connection: close
Content-Type: text/html
```

Recommendations

We are currently unaware of a practical solution to this problem. Please consider the following workarounds.

Some of these mitigations may protect entire applications, while others may only protect individual web pages.

- Disable HTTP compression.

- Separate the secrets from the user input.

- Randomize the secrets in each client request.

- Mask secrets (effectively randomizing by XORing with a random secret per request).

- Protect web pages from CSRF attacks.

- Obfuscate the length of web responses by adding random amounts of arbitrary bytes.

2.1.4. Informational findings

2.1.4.1 ICMP Address Mask and/or Timestamp Requests Allowed From Arbitrary Hosts

Vulnerability status: Unattended

Description

Remote server responds to ICMP timestamp and/or address mask requests.

ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts. This method of attack provides information that could help an attacker to identify other vulnerabilities, but does no direct harm.

The informational finding is based on the following retrieved information from 0/ICMP:

```
Remote host responds to ICMP Timestamp Request
```

Recommendations

Configure your firewall to block ICMP packets of type 13/17 or disable ICMP replies for type 13/17 on your system.

Tags

Informational

External references

CVE-1999-0524

2.1.4.2 Ping the remote host

Vulnerability status: Unattended

Description

This plugin checks if the remote host responses to ping.

This plugin checks if the remote host is alive using one or more ping types:

- An ARP ping, if the host is on the local subnet

- An ICMP ping

- A TCP ping, which sends a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK

- A UDP ping (DNS, RPC, NTP, etc.)

The informational finding is based on the following retrieved information from 0/ICMP:

```
The remote host replied to an ICMP ping packet
```

Recommendations

This finding is informational, no action is required.

Tags

Informational

2.1.4.3 robots.txt was not found

Vulnerability status: Unattended

Description

The robots.txt file was not found on the remote host.

The robots.txt file is used to give instructions to web robots also known as search engines such as Google, Bing and others. The file defines what content web robots are allowed to index, which robots you allow and much more.

When robots.txt does not exist, web robots will attempt to index the web application. In that case, ensure that the web application do not expose any sensitive information.

For more information please see the following references:

- List of web robots http://www.robotstxt.org/db.html

- Paper about robots.txt http://www.sans.org/reading_room/whitepapers/awareness/robotstxt_33955

The informational finding is based on the following retrieved information from 443/TCP:

```
The robots.txt file is not available on the remote host
```

Recommendations

Define rules for web robots and add robots.txt file.

Tags

Informational

2.1.4.4 Service Detected: WWW (Apache HTTP Server)

Vulnerability status: Unattended

Description

The remote host is running Apache HTTP Server.

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards. The Apache HTTP Server is a project of The Apache Software Foundation.

The informational finding is based on the following retrieved information from 443/TCP:

```
Apache HTTP Server is running on this port.
Banner:
HTTP/1.1 200 OK
Date: Wed, 04 Jan 2017 09:12:07 GMT
Server: Apache/2.2.16 (Ubuntu)
Last-Modified: Tue, 16 Jul 2013 12:32:17 GMT
ETag: "22e71-b1-4e1a02aec6c24"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

Recommendations

This finding is informational, no action is required.

Tags

Apache, Informational, Service detection, Web Server

2.1.4.5 SSL server certificate test

Vulnerability status: Unattended

Description

This is information about remote server's SSL Certificate.

The SSL certificate's validity is checked for security flaws and misconfigurations. For more information please see the findings below.

Note that you must scan a FQDN (fully qualified domain name) and not the IP address in order obtain reliable results.

The informational finding is based on the following retrieved information from 443/TCP:

```
The certificate expires on 20-07-2023 09:22:09 AM and this date is in the future.

The certificate is valid since 22-07-2013 09:22:09 AM and this date is in the
past.

The signing algorithm used for this algorithm is considered as strong (OID:
1.2.840.113549.1.1.5 name: sha1WithRsaEncryption).

This is the SSL certificate provided by the service:
[Subject]
CN=localhost

[Issuer]
CN=localhost

[Serial Number]
00B990D457D558006E

[Not Before]
22-07-2013 09:22:09

[Not After]
20-07-2023 09:22:09

[Thumbprint]
5AD2DBC85CE9DA5531B8DD464B294663E8D60172
```

Recommendations

Review your certificate and regenerate it if necessary

Tags

Informational, SSL, TLS

2.1.4.6 SSL/TLS CBC mode ciphers information disclosure (BEAST attack)

Vulnerability status: Unattended

Description

The remote web server could be affected by an information disclosure vulnerability.

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which 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.

In order to perform a successful attack the following requirements must be met:

1) The attacker must eavesdrop on connections made from the victim's browser.

2) The attack must inject JavaScript into the victim's browser.

3) The attacker must send HTTPS requests at will.

4) After listening in on the request, the attack must be append more data to the very same request.

It is a browser-side vulnerability and it was mitigated with all major browsers.

The informational finding is based on the following retrieved information from 443/TCP:

```
BEAST is not mitigated server-side.
```

Recommendations

Server-side: Upgrade to TLS 1.2 or higher (this may raise compatibility issues).

Client-side remediation: (apart from upgrading the protocol to TLS 1.2 or higher) is implementing 1/n-1 record splitting. This would allow using CBC ciphers safely even with older protocol versions.

Tags

Informational, SSL, TLS

External references

CVE-2011-3389

http://www.securityfocus.com/bid/49388

2.1.4.7 SSL/TLS secure renegotiation is supported

Vulnerability status: Unattended

Description

The remote server supports secure SSL/TLS renegotiation.

The remote server supports secure SSL/TLS renegotiation.

The informational finding is based on the following retrieved information from 443/TCP:

```
Secure renegotiation is supported
```

Recommendations

This finding is informational, no action is required.

Tags

Informational, SSL, TLS

2.1.4.8 SSL/TLS supported cipher suites enumeration

Vulnerability status: Unattended

Description

Identify SSL/TLS cipher suites.

This plugin enumerates available SSL/TLS cipher suites.

The informational finding is based on the following retrieved information from 443/TCP:

```
Cipher Suites (Server has no preference):

SSL3:
TLS_RSA_WITH_RC4_128_MD5 [RC4-MD5]
TLS_RSA_WITH_RC4_128_SHA [RC4-SHA]
TLS_RSA_WITH_3DES_EDE_CBC_SHA [DES-CBC3-SHA]
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA [EDH-RSA-DES-CBC3-SHA]
TLS_RSA_WITH_AES_128_CBC_SHA [AES128-SHA]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA [DHE-RSA-AES128-SHA]
TLS_RSA_WITH_AES_256_CBC_SHA [AES256-SHA]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA [DHE-RSA-AES256-SHA]

TLS1:
TLS_RSA_WITH_RC4_128_MD5 [RC4-MD5]
TLS_RSA_WITH_RC4_128_SHA [RC4-SHA]
TLS_RSA_WITH_3DES_EDE_CBC_SHA [DES-CBC3-SHA]
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA [EDH-RSA-DES-CBC3-SHA]
TLS_RSA_WITH_AES_128_CBC_SHA [AES128-SHA]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA [DHE-RSA-AES128-SHA]
TLS_RSA_WITH_AES_256_CBC_SHA [AES256-SHA]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA [DHE-RSA-AES256-SHA]
```

Recommendations

This finding is informational, no action is required.

Tags

Informational, SSL, TLS

2.1.4.9 Web Application Detected: GLPI

Vulnerability status: Unattended

Description

The remote host contains GLPI, the Information Resource-Manager with an additional Administration- Interface.

The remote host is running GLPI, the Information Resource-Manager with an additional Administration- Interface.

The informational finding is based on the following retrieved information from 443/TCP:

```
The remote host is running GLPI: https://10.50.2.161:443/glpi/
```

Recommendations

This finding is informational, no action is required.

Tags

Informational, Web application

2.1.4.10 Web Application Detected: phpMyAdmin

Vulnerability status: Unattended

Description

phpMyAdmin was found installed on the target web server.

phpMyAdmin was detected.

The informational finding is based on the following retrieved information from 443/TCP:

```
The remote host is running phpMyAdmin: https://10.50.2.161:443/phpmyadmin/

Version: 3.3.7
```

Recommendations

This finding is informational, no action is required.

Tags

Informational, Web application

2.1.4.11 Web Application Detected: TaskFreak

Vulnerability status: Unattended

Description

The remote host contains TaskFreak, an open source project management web application.

The remote host is running TaskFreak, an open source project management web application.

The informational finding is based on the following retrieved information from 443/TCP:

```
The remote host is running TaskFreak: https://10.50.2.161:443/taskfreak/

Version: 0.6.1
```

Recommendations

This finding is informational, no action is required.

Tags

Informational, Web application

2.1.4.12 Web Application Detected: Wordpress

Vulnerability status: Unattended

Description

Wordpress was found installed on the target web server.

Wordpress was detected.

The informational finding is based on the following retrieved information from 443/TCP:

```
The remote host is running Wordpress: https://10.50.2.161:443/wordpress/

Version: 3.5.2
```

Recommendations

This finding is informational, no action is required.

Tags

Informational, Web application

2.1.5. Potential vulnerabilities

2.1.5.1 Apache HTTP Server mod_proxy_ajp Module Denial of Service Vulnerability

Medium AV: **Network** AC: **Low** Au: **None** C: **None** I: **None** A: **Partial** **5.0**

Vulnerability status: Unattended

Description

The remote web server is affected by a denial of service vulnerability.

The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version.

Tags

Apache, Version Based, Web Server

External references

CVE-2012-4557

2.1.5.2 Apache HTTP Server 'ap_pregsub()' Function Local Privilege Escalation Vulnerability

Medium AV: **Local** AC: **Medium** Au: **None** C: **Partial** I: **Partial** A: **Partial** **4.4**

Vulnerability status: Unattended

Description

The remote web server is affected by a local privilege escalation vulnerability.

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version.

Workaround: disable the module when not needed or disable use of .htaccess on all user-modificable locations by setting AllowOverride None on all corresponding directories

Tags

Apache, Version Based, Web Server

External references

CVE-2011-3607

http://www.securityfocus.com/bid/50494

2.1.5.3 Apache HTTP Server before 2.2.18 Stack Consumption Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **None** A: **Partial** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by a stack consumption vulnerability.

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest version of Apache or disable the 'mod_autoindex' module.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-0419

2.1.5.4 Apache HTTP Server mod_proxy Module Request Bypass of the Reverse Proxy Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by a security bypass vulnerability.

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-3639

2.1.5.5 Apache HTTP Server Uri Scheme Bypass of the Reverse Proxy Vulnerability

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by a security bypass vulnerability.

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-4317

http://www.securityfocus.com/archive/1/archive/1/535181/100/0/threaded

2.1.5.6 Apache MPM-ITK Module Security Weakness

Medium AV: **Network** AC: **Medium** Au: **None** C: **None** I: **Partial** A: **None** **4.3**

Vulnerability status: Unattended

Description

The remote web server is affected by a privileges escalation vulnerability.

The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

Upgrade to the latest Apache version.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-1176

http://www.securityfocus.com/bid/46953

2.1.5.7 Apache HTTP Server Local Denial Of Service Vulnerability

Low AV: **Local** AC: **High** Au: **None** C: **None** I: **None** A: **Partial** **1.2**

Vulnerability status: Unattended

Description

The remote web server is affected by a local denial of service vulnerability.

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.

The vulnerability is based on the following retrieved information from 443/TCP:

```
Apache/2.2.16 (Ubuntu)
```

Recommendations

It is strongly recommended to upgrade the Apache server to the latest stable version.

Workaround: disable the module when not needed or disable use of .htaccess on all user-modificable locations by setting AllowOverride None on all corresponding directories.

Tags

Apache, Version Based, Web Server

External references

CVE-2011-4415

3. APPENDIX

3.1. About test methodology

The complexity of expanded infrastructures and modern IT solutions triggers the need of complete, deep and well-balanced security assessments. To face this challenge, F-Secure has developed a proprietary methodology aiming to evaluate the security of the requested environments.

In general, the vulnerability scanning process consists of four phases.

3.1.1. Reconnaissance

This phase gives a very general overview of the target environment. The goal is to figure out what kind of components and services are present in the infrastructure. The information about the targets (hosts, URLs, credentials) may be collected by various means such as, WHOIS databases, and DNS including white intelligence techniques as well as the input given by the customer. Moreover, network discovery using F-Secure's proprietary network scanner, F-Secure Radar Discovery Scan, is performed in order to identify systems present in customer's networks.

3.1.2. Enumeration

During this phase, the information gathered in the previous step is utilized to steer the more detailed scanning against individual components and services. The platform scan is performed with F-Secure Radar System Scan. The web applications are scanned using the F-Secure Radar Web Scanner.

3.1.3. Research for vulnerabilities and (optional) exploitation

This is an optional and manual phase where the F-Secure Radar user put in most of the effort. The vulnerabilities identified in the previous phase need to be thoroughly verified to avoid (as much as it is possible) false positives and provide appropriate quality of the results.

3.1.4. Reporting

The final phase is reporting, the process of documenting all of the vulnerabilities identified during the assessment. Every finding is documented with a detailed description including the exact location, conditions when the vulnerability occurs (together with information allowing the customer to reproduce the finding), security impact analysis, and proposed remediation strategy. The goal is to provide both detailed and precise information about security issues, but also to suggest the best way to mitigate them.

F-Secure Radar has a powerful reporting engine that allows the end-user to customize the content of the report and download reports in various formats.

3.2. About CVSS scoring

The findings are scored using the international CVSSv2 metrics. The goal of the scoring system is to find common metrics for the findings. Using a common scoring system allows comparison of findings between assignments. It is worth noting however, that the numerical value (CVSSv2 score) is only meant for general guidance and should be interpreted as such.

3.2.1. About base metrics

The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability. For example, a vulnerability could cause a partial loss of integrity and availability, but no loss of confidentiality.

3.2.2. Access Vector (AV)

This metric reflects how the vulnerability is exploited. The possible values for this metric are listed in the table below. The more remote an attacker can be to attack a host, the greater the vulnerability score.

3.2.2.1 Local (L)

A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g., sudo).

3.2.2.2 Adjacent Network (A)

A vulnerability exploitable with *adjacent network access* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment.

3.2.2.3 Network (N)

A vulnerability exploitable with *network access* means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable". An example of a network attack is an RPC buffer overflow.

3.2.3. Access Complexity (AC)

This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. For example, consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will.

3.2.3.1 High (H)

Specialized access conditions exist. For example:

- In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (e.g., DNS hijacking).
- The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions.
- The vulnerable configuration is seen very rarely in practice.
- If a race condition exists, the window is very narrow.

3.2.3.2 Medium (M)

The access conditions are somewhat specialized; the following are examples:

- The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted.
- Some information must be gathered before a successful attack can be launched.
- The affected configuration is non-default, and is not commonly configured (e.g., a vulnerability present when a server performs user account authentication via a specific scheme, but not present for another authentication scheme).
- The attack requires a small amount of social engineering that might occasionally fool cautious users (e.g., phishing attacks that modify a web browsers status bar to show a false link, having to be on someones buddy list before sending an IM exploit).

3.2.3.3 Low (L)

Specialized access conditions do not exist. The following are examples:

- The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server).
- The affected configuration is default or ubiquitous.
- The attack can be performed manually and requires little skill or additional information gathering.
- The race condition is a lazy one (i.e., it is technically a race but easily winnable).

3.2.4. Authentication (Au)

This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur. The possible values for this metric are listed in Table 3. The fewer authentication instances that are required, the higher the vulnerability score.

3.2.4.1 Multiple (M)

Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. An example is an attacker authenticating to an operating system in addition to providing credentials to access an application hosted on that system.

3.2.4.2 Single (S)

The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).

3.2.4.3 None (N)

Authentication is not required to exploit the vulnerability.

3.2.5. Confidentiality Impact (C)

This metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The possible values for this metric are listed in Table 4. Increased confidentiality impact increases the vulnerability score.

3.2.5.1 None (N)

There is no impact to the confidentiality of the system.

3.2.5.2 Partial (P)

There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database.

3.2.5.3 Complete (C)

There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.)

3.2.6. Integrity Impact (I)

3.2.6.1 None (N)

There is no impact to the integrity of the system.

3.2.6.2 Partial (P)

Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope.

3.2.6.3 Complete (C)

There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

3.2.7. Availability Impact (A)

3.2.7.1 None (N)

There is no impact to the availability of the system.

3.2.7.2 Partial (P)

There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.

3.2.7.3 Complete (C)

There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

3.2.8. Total severity ranking

CVSSv2 provides severity rankings of "Low," "Medium," and "High" in addition to the numeric scores. These qualitative rankings are mapped from the numeric scores.

Severity CVSS score	**Low** 0.0 – 3.9	**Medium** 4.0 – 6.9	**High** 7.0 – 10.0

For more information, please refer to: http://www.first.org/cvss/cvss-guide.html