Remediation Plan

comsics.usm.my

Audited on August 7, 2019

Reported on August 7, 2019

1. Discovered Systems

Node	Operating System	Risk	Aliases
10.205.19.208	CentOS Linux	53,329	

2. Risk Assessment

This report identifies security risks that could adversely affect your critical operations and assets. These risks are quantified according to their likelihood of occurrence and the potential damage if they occur. Risk factors are combined to form an overall risk index for each system, allowing you to prioritize your remediation activities accordingly.

Risk strategy: Real Risk. This strategy analyzes potential types of exposures associated with vulnerabilities to expand and deepen your understanding of real threats to your environment and the value of different mitigation approaches. The algorithm applies exploit and malware exposure metrics for each vulnerability to CVSS base metrics for asset impact (confidentiality, integrity, and availability) and likelihood of compromise (access vector, access complexity, and authentication requirements). It also indicates how time increases likelihood.

Device	Risk Index	Risk Factors
10.205.19.208	53,329	•This device is in the comsics.usm.my site with normal importance. •14 critical vulnerabilities were discovered. •157 severe vulnerabilities were discovered. •9 moderate vulnerabilities were discovered. •2 NFS services were discovered. •One HTTP service was discovered. •One SSH service was discovered.

3. Remediation Plan

3.1. Remediation Plan for 10.205.19.208

3.1.1. For Wordpress 3.1.3

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 3 hours.

Upgrade to the latest version of Wordpress

Estimated time: 3 hours

Wordpress Wordpress

Upgrade to the latest version of Wordpress from https://wordpress.org/download/release-archive/

This will address the following 159 issues:

- Wordpress: CVE-2012-0287: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2012-0287)
- Wordpress: CVE-2012-2402: Permissions, Privileges, and Access Controls (wordpress-cve-2012-2402)
- Wordpress: CVE-2012-2403: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2012-2403)
- Wordpress: CVE-2012-2404: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2012-2404)
- Wordpress: CVE-2012-3383: Permissions, Privileges, and Access Controls (wordpress-cve-2012-3383)
- Wordpress: CVE-2012-3384: Cross-Site Request Forgery (CSRF) (wordpress-cve-2012-3384)
- Wordpress: CVE-2012-3385: Permissions, Privileges, and Access Controls (wordpress-cve-2012-3385)
- Wordpress: CVE-2012-3414: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2012-3414)
- Wordpress: CVE-2012-4421: Permissions, Privileges, and Access Controls (wordpress-cve-2012-4421)
- Wordpress: CVE-2012-4422: Permissions, Privileges, and Access Controls (wordpress-cve-2012-4422)
- Wordpress: CVE-2012-4448: Cross-Site Request Forgery (CSRF) (wordpress-cve-2012-4448)
- Wordpress: CVE-2012-6633: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2012-6633)
- Wordpress: CVE-2012-6634: Permissions, Privileges, and Access Controls (wordpress-cve-2012-6634)
- Wordpress: CVE-2012-6635: Permissions, Privileges, and Access Controls (wordpress-cve-2012-6635)
- Wordpress: CVE-2012-6707: Inadequate Encryption Strength (wordpress-cve-2012-6707)
- Wordpress: CVE-2013-0235: Unspecified Security Vulnerability (wordpress-cve-2013-0235)
- Wordpress: CVE-2013-0236: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2013-0236)
- Wordpress: CVE-2013-0237: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2013-0237)
- Wordpress: CVE-2013-2173: Cryptographic Issues (wordpress-cve-2013-2173)
- Wordpress: CVE-2013-2199: Permissions, Privileges, and Access Controls (wordpress-cve-2013-2199)
- Wordpress: CVE-2013-2200: Permissions, Privileges, and Access Controls (wordpress-cve-2013-2200)

- Wordpress: CVE-2013-2201: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2013-2201)
- Wordpress: CVE-2013-2202: Information Exposure (wordpress-cve-2013-2202)
- Wordpress: CVE-2013-2203: Permissions, Privileges, and Access Controls (wordpress-cve-2013-2203)
- Wordpress: CVE-2013-2204: Improper Input Validation (wordpress-cve-2013-2204)
- Wordpress: CVE-2013-2205: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2013-2205)
- Wordpress: CVE-2013-4338: Improper Control of Generation of Code ('Code Injection') (wordpress-cve-2013-4338)
- Wordpress: CVE-2013-4339: Improper Input Validation (wordpress-cve-2013-4339)
- Wordpress: CVE-2013-4340: Permissions, Privileges, and Access Controls (wordpress-cve-2013-4340)
- Wordpress: CVE-2013-5738: Improper Input Validation (wordpress-cve-2013-5738)
- Wordpress: CVE-2013-5739: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2013-5739)
- Wordpress: CVE-2014-5203: Unspecified Security Vulnerability (wordpress-cve-2014-5203)
- Wordpress: CVE-2014-5204: Cross-Site Request Forgery (CSRF) (wordpress-cve-2014-5204)
- Wordpress: CVE-2014-5205: Cross-Site Request Forgery (CSRF) (wordpress-cve-2014-5205)
- Wordpress: CVE-2014-5240: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2014-5240)
- Wordpress: CVE-2014-6412: Weak Password Recovery Mechanism for Forgottentlfjidkuuklkvrndhhnhcgdvgcbgkrklvbcrtlrblkgb Password (wordpress-cve-2014-6412)
- Wordpress: CVE-2014-9033: Cross-Site Request Forgery (CSRF) (wordpress-cve-2014-9033)
- 4 instances of Wordpress: CVE-2014-9034: Data Processing Errors (wordpress-cve-2014-9034)
- 4 instances of Wordpress: CVE-2014-9035: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2014-9035)
- 4 instances of Wordpress: CVE-2014-9036: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2014-9036)
- 4 instances of Wordpress: CVE-2014-9037: Cryptographic Issues (wordpress-cve-2014-9037)
- 4 instances of Wordpress: CVE-2014-9038: Improper Input Validation (wordpress-cve-2014-9038)
- 4 instances of Wordpress: CVE-2014-9039: Security Features (wordpress-cve-2014-9039)
- Wordpress: CVE-2015-2213: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (wordpress-cve-2015-2213)
- Wordpress: CVE-2015-3438: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-3438)
- Wordpress: CVE-2015-3439: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-3439)
- Wordpress: CVE-2015-3440: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-3440)
- Wordpress: CVE-2015-5622: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-5622)
- Wordpress: CVE-2015-5623: Improper Access Control (wordpress-cve-2015-5623)

- Wordpress: CVE-2015-5714: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-5714)
- Wordpress: CVE-2015-5715: Permissions, Privileges, and Access Controls (wordpress-cve-2015-5715)
- Wordpress: CVE-2015-5730: Information Exposure (wordpress-cve-2015-5730)
- Wordpress: CVE-2015-5731: Cross-Site Request Forgery (CSRF) (wordpress-cve-2015-5731)
- Wordpress: CVE-2015-5732: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-5732)
- Wordpress: CVE-2015-5733: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-5733)
- Wordpress: CVE-2015-5734: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-5734)
- Wordpress: CVE-2015-7989: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-7989)
- Wordpress: CVE-2015-8834: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2015-8834)
- Wordpress: CVE-2016-10148: Improper Access Control (wordpress-cve-2016-10148)
- Wordpress: CVE-2016-1564: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-1564)
- Wordpress: CVE-2016-2221: Unspecified Security Vulnerability (wordpress-cve-2016-2221)
- Wordpress: CVE-2016-2222: Unspecified Security Vulnerability (wordpress-cve-2016-2222)
- Wordpress: CVE-2016-4029: Improper Authorization (wordpress-cve-2016-4029)
- Wordpress: CVE-2016-4566: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-4566)
- Wordpress: CVE-2016-4567: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-4567)
- Wordpress: CVE-2016-5832: Unspecified Security Vulnerability (wordpress-cve-2016-5832)
- Wordpress: CVE-2016-5833: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-5833)
- Wordpress: CVE-2016-5834: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-5834)
- Wordpress: CVE-2016-5835: Information Exposure (wordpress-cve-2016-5835)
- Wordpress: CVE-2016-5836: Unspecified Security Vulnerability (wordpress-cve-2016-5836)
- Wordpress: CVE-2016-5837: Unspecified Security Vulnerability (wordpress-cve-2016-5837)
- Wordpress: CVE-2016-5838: Credentials Management (wordpress-cve-2016-5838)
- Wordpress: CVE-2016-5839: Unspecified Security Vulnerability (wordpress-cve-2016-5839)
- Wordpress: CVE-2016-6634: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-6634)
- Wordpress: CVE-2016-6635: Cross-Site Request Forgery (CSRF) (wordpress-cve-2016-6635)
- Wordpress: CVE-2016-6896: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (wordpress-cve-2016-6896)

- Wordpress: CVE-2016-6897: Cross-Site Request Forgery (CSRF) (wordpress-cve-2016-6897)
- Wordpress: CVE-2016-7168: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2016-7168)
- Wordpress: CVE-2016-7169: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (wordpress-cve-2016-7169)
- Wordpress: CVE-2016-9263: Improper Input Validation (wordpress-cve-2016-9263)
- Wordpress: CVE-2017-1000600: Improper Input Validation (wordpress-cve-2017-1000600)
- Wordpress: CVE-2017-14718: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-14718)
- Wordpress: CVE-2017-14719: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (wordpress-cve-2017-14719)
- Wordpress: CVE-2017-14720: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-14720)
- Wordpress: CVE-2017-14721: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-14721)
- Wordpress: CVE-2017-14722: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (wordpress-cve-2017-14722)
- Wordpress: CVE-2017-14723: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (wordpress-cve-2017-14723)
- Wordpress: CVE-2017-14724: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-14724)
- Wordpress: CVE-2017-14725: URL Redirection to Untrusted Site ('Open Redirect') (wordpress-cve-2017-14725)
- Wordpress: CVE-2017-14726: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-14726)
- Wordpress: CVE-2017-14990: Information Exposure (wordpress-cve-2017-14990)
- Wordpress: CVE-2017-16510: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (wordpress-cve-2017-16510)
- Wordpress: CVE-2017-17091: Improper Access Control (wordpress-cve-2017-17091)
- Wordpress: CVE-2017-17092: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-17092)
- Wordpress: CVE-2017-17093: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-17093)
- Wordpress: CVE-2017-17094: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-17094)
- Wordpress: CVE-2017-5487: Information Exposure (wordpress-cve-2017-5487)
- Wordpress: CVE-2017-5488: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-5488)
- Wordpress: CVE-2017-5489: Cross-Site Request Forgery (CSRF) (wordpress-cve-2017-5489)
- Wordpress: CVE-2017-5490: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-5490)

- Wordpress: CVE-2017-5491: Security Features (wordpress-cve-2017-5491)
- Wordpress: CVE-2017-5492: Cross-Site Request Forgery (CSRF) (wordpress-cve-2017-5492)
- Wordpress: CVE-2017-5493: Cryptographic Issues (wordpress-cve-2017-5493)
- Wordpress: CVE-2017-5610: Information Exposure (wordpress-cve-2017-5610)
- Wordpress: CVE-2017-5611: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (wordpress-cve-2017-5611)
- Wordpress: CVE-2017-5612: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-5612)
- Wordpress: CVE-2017-6814: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-6814)
- Wordpress: CVE-2017-6815: Improper Input Validation (wordpress-cve-2017-6815)
- Wordpress: CVE-2017-6816: Improper Access Control (wordpress-cve-2017-6816)
- Wordpress: CVE-2017-6817: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-6817)
- Wordpress: CVE-2017-6818: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-6818)
- Wordpress: CVE-2017-6819: Cross-Site Request Forgery (CSRF) (wordpress-cve-2017-6819)
- Wordpress: CVE-2017-9061: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-9061)
- Wordpress: CVE-2017-9062: Data Processing Errors (wordpress-cve-2017-9062)
- Wordpress: CVE-2017-9063: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2017-9063)
- Wordpress: CVE-2017-9064: Cross-Site Request Forgery (CSRF) (wordpress-cve-2017-9064)
- Wordpress: CVE-2017-9065: Improper Input Validation (wordpress-cve-2017-9065)
- Wordpress: CVE-2017-9066: Server-Side Request Forgery (SSRF) (wordpress-cve-2017-9066)
- Wordpress: CVE-2018-1000773: Improper Input Validation (wordpress-cve-2018-1000773)
- Wordpress: CVE-2018-10100: URL Redirection to Untrusted Site ('Open Redirect') (wordpress-cve-2018-10100)
- Wordpress: CVE-2018-10101: URL Redirection to Untrusted Site ('Open Redirect') (wordpress-cve-2018-10101)
- Wordpress: CVE-2018-10102: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2018-10102)
- Wordpress: CVE-2018-12895: Wordpress Authenticated Arbitrary File Deletion (wordpress-cve-2018-12895)
- 2 instances of Wordpress: CVE-2018-20147: Improper Access Control (wordpress-cve-2018-20147)
- Wordpress: CVE-2018-20148: Deserialization of Untrusted Data (wordpress-cve-2018-20148)
- 2 instances of Wordpress: CVE-2018-20149: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2018-20149)
- 2 instances of Wordpress: CVE-2018-20150: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2018-20150)
- 2 instances of Wordpress: CVE-2018-20151: Information Exposure (wordpress-cve-2018-20151)
- Wordpress: CVE-2018-20152: Improper Input Validation (wordpress-cve-2018-20152)
- 2 instances of Wordpress: CVE-2018-20153: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2018-20153)

•Wordpress: CVE-2018-5776: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (wordpress-cve-2018-5776)
•Wordpress: CVE-2018-6389: Uncontrolled Resource Consumption ('Resource Exhaustion') (wordpress-cve-2018-6389)
•2 instances of Wordpress: CVE-2019-8942: Improper Control of Generation of Code ('Code Injection') (wordpress-cve-2019-8942)
•Wordpress: CVE-2019-9787: Cross-Site Request Forgery (CSRF) (wordpress-cve-2019-9787)
•Obsolete Version of WordPress (wordpress-obsolete)

3.1.2. For Apache HTTPD 2.2.15

These vulnerabilities can be resolved by performing the following 5 steps. The total estimated time to perform all of these steps is 5 hours 50 minutes.

Upgrade to the latest version of Apache HTTPD

Estimated time: 2 hours
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.39.tar.gz
The latest version of Apache HTTPD is 2.4.39.
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.
This will address the following 36 issues:
•Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)
•Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)
•Apache HTTPD: mod_cache and mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)
•Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)
•Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)
•Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)
•Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)
•Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)
•Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)
•Apache HTTPD: Potential pattern expansion problem when mod-proxy and mod-rewrite are used together (CVE-2011-3639) (apache-httpd-cve-2011-3639)
•Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)
•Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)
•Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)
•Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)
•Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apache-httpd-cve-2012-2687)
•Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)
•Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)
•Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)
•Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)
•Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)
•Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704) (apache-httpd-cve-2013-5704)
•Apache HTTPD: mod_dav crash (CVE-2013-6438) (apache-httpd-cve-2013-6438)

•Apache HTTPD: mod_log_config crash (CVE-2014-0098) (apache-httpd-cve-2014-0098)
•Apache HTTPD: mod_deflate denial of service (CVE-2014-0118) (apache-httpd-cve-2014-0118)
•Apache HTTPD: mod_status buffer overflow (CVE-2014-0226) (apache-httpd-cve-2014-0226)
•Apache HTTPD: mod_cgid denial of service (CVE-2014-0231) (apache-httpd-cve-2014-0231)
•Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183) (apache-httpd-cve-2015-3183)
•Apache HTTPD: mod_userdir CRLF injection (CVE-2016-4975) (apache-httpd-cve-2016-4975)
•Apache HTTPD: HTTP_PROXY environment variable "httpoxy" mitigation (CVE-2016-5387) (apache-httpd-cve-2016-5387)
•Apache HTTPD: Apache HTTP Request Parsing Whitespace Defects (CVE-2016-8743) (apache-httpd-cve-2016-8743)
•Apache HTTPD: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167) (apache-httpd-cve-2017-3167)
•Apache HTTPD: mod_ssl Null Pointer Dereference (CVE-2017-3169) (apache-httpd-cve-2017-3169)
•Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679) (apache-httpd-cve-2017-7679)
•Apache HTTPD: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788) (apache-httpd-cve-2017-9788)
•Apache HTTPD: Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798) (apache-httpd-cve-2017-9798)
•Obsolete Version of Apache HTTPD (apache-httpd-obsolete)

Disable HTTP TRACE Method for Apache

Estimated time: 2 hours
Apache HTTPD
Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:
TraceEnable off
For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
This will address the following issue: HTTP TRACE Method Enabled (http-trace-method-enabled).

Disable inode-based ETag generation in the Apache config

Estimated time: 1 hour
You can remove inode information from the ETag header by adding the following directive to your Apache config:

```
FileETag MTime Size
```

This will address the following issue: Apache HTTPD: ETag Inode Information Leakage (CVE-2003-1418) (apache-httpd-cve-2003-1418).

Disable HTTP OPTIONS Method for Apache

Estimated time: 30 minutes
Apache HTTPD
Disable the OPTIONS method by including the following in the Apache configuration:

```
<Limit OPTIONS>
 Order deny,allow
 Deny from all
</Limit>
```

This will address the following issue: HTTP OPTIONS Method Enabled (http-options-method-enabled).

Disable HTTP OPTIONS method

Estimated time: 20 minutes

Disable HTTP OPTIONS method on your web server. Refer to your web server's instruction manual on how to do this.

Web servers that respond to the OPTIONS HTTP method expose what other methods are supported by the web server, allowing attackers to narrow and intensify their efforts.

This will address the following issue: HTTP OPTIONS Method Enabled (http-options-method-enabled).

3.1.3. General

These vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 15 minutes.

No fixes or workaround suggested by the vendor

Estimated time: 0 seconds

No fixes or workaround suggested by the vendor. Disable or restrict access to the endpoint until a solution is available

This will address the following 3 issues:

- Wordpress: CVE-2017-8295: Weak Password Recovery Mechanism for Forgotten Password (wordpress-cve-2017-8295)
- Wordpress: CVE-2018-14028: Unrestricted Upload of File with Dangerous Type (wordpress-cve-2018-14028)
- Wordpress: CVE-2019-8943: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (wordpress-cve-2019-8943)

Perform firewalling or filtering

Estimated time: 15 minutes

Many vendors do not consider this to be a vulnerability, or a vulnerability worth fixing, so there are no vendor-provided solutions aside from putting a firewall or other filtering device between the target and hostile attackers that is capable of randomizing IP IDs.

This will address the following issue: UDP IP ID Zero (udp-ipid-zero).

3.1.4. For CentOS Linux

These vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 35 minutes.

Disable TCP timestamp responses on Linux

Estimated time: 5 minutes

Linux

Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.ipv4.tcp_timestamps=0
```

This will address the following issue: TCP timestamp response (generic-tcp-timestamp).

Disable ICMP timestamp responses on Linux

Estimated time: 30 minutes

Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

This will address the following issue: ICMP timestamp response (generic-icmp-timestamp).