

Vulnerability remediation report for Lab Network (demo)

PREPARED FOR	PREPARED BY	SCAN DATE	STATUS
Lab Network (demo)	Varaxon Technologies	2026-09-05	No exploitation intelligence

Executive summary

The scan found outdated software and weak encryption settings on this host that need planned work, though it is only a point-in-time view from one position.

We scanned 1 host. The scanner reported 459 distinct findings on 1 of 1 hosts, giving 493 vulnerable instances. The scan date recorded in the export is 2026-09-05.

Most findings sit in Band 5, which covers issues with no CVE identifier but a rating of 2 or above. Band 6 holds 90 low or informational findings. Bands 1 to 4 hold 0, 0, 0 and 0 findings respectively. Because no CVE identifiers were recorded, we could not check these findings against CISA's Known Exploited Vulnerabilities (KEV) catalog, so their exploitation status is unknown, not known to be absent.

The work is grouped into campaigns by team. The PHP upgrade covers the largest group of findings and needs a planned web service restart, so it should be scheduled first. We will rescan after each change to confirm it took effect.

Key points

- Most of the work is in old web software on this host: PHP, Apache HTTP Server and phpMyAdmin.
- Several fixes need a restart, a change window or application testing before they go live.
- Exploitation status is unknown for these findings because the export carries no CVE identifiers.
- Mail and database ports use weak encryption settings and an expired certificate, reported by the scanner.
- A scan cannot show that a system is free of vulnerabilities; it shows what the scanner could check at the time.

Decisions for leadership

- Approve a planned change window with a web service restart for the PHP and Apache upgrades.
- Decide whether Apache moves to the newer 2.4 line, which needs application testing, or to the 2.2 line with a smaller change.
- Approve disabling the legacy rlogin service once the system owner confirms no user depends on it.
- Approve the time needed to check the FTP server for signs of compromise before any reinstall.
- Decide how to handle the lower-priority items and the manual review item, which can follow the main campaigns.

Findings at a glance

Findings by priority band

● Band 1	KEV + ransomware	0
● Band 2	KEV	0
● Band 3	urgent CVSS, no KEV match	0
● Band 4	has CVE, non-trivial severity	0
● Band 5	no CVE, non-trivial severity	369
● Band 6	low or informational	90

1

hosts with findings

1

hosts scanned

459

distinct findings

unknown

known exploited
(KEV)

332

remediation actions

Remediation plan

Band 5 Upgrade PHP on the web server to a supported release

Actions 2, 4, 5, 6, 33, 37, 38, 39, 41

PHP is the largest group of findings on this host. The scanner lists several target versions, and the highest one covers the lower targets, so a single planned upgrade is the efficient fix. Application testing matters because the change spans a large jump in PHP versions.

Steps in order:

1. Confirm with the application owner which PHP release the site needs. The export does not show whether the target release is still supported, so check the vendor's support dates before choosing it.
2. Back up the web site files and the PHP configuration before the change.
3. Test the site and its applications on a copy of the host using PHP 7.2.29 or a later release. The scanner states minimums, so a later release may be needed.
4. Schedule a web service restart on TCP port 80 in a change window, then install the chosen PHP release on `metasploitable2.greenbone-community-edition_default` and restart the service.
5. Verify by checking the installed PHP version on `metasploitable2.greenbone-community-edition_default` and rescanning the PHP checks. Each should no longer report on TCP port 80.

Restarting the web service causes a planned outage of the site on TCP port 80. Plan the window and tell users in advance.

Band 5 Update phpMyAdmin and check it on the new PHP release

Actions 7, 26, 27, 31

phpMyAdmin is a database administration web tool. The scanner reported cross-site scripting and SQL injection weaknesses in it. Its upgrade should follow the PHP change, because phpMyAdmin runs on PHP.

Steps in order:

1. Confirm where phpMyAdmin is installed on `metasploitable2.greenbone-community-edition_default`, since the export does not show its location.
2. Upgrade to phpMyAdmin 4.9.2 or later. For some reported items the scanner's version text could not be read, so confirm the target in the phpMyAdmin release notes before installing.
3. Test sign-in and the main pages after the change.
4. Verify by checking the version shown on the phpMyAdmin page and rescanning the phpMyAdmin checks on TCP port 80.

The PHP and phpMyAdmin changes should share one change window, since a PHP restart may be needed after this change.

Band 5 Update Apache HTTP Server on the web server

Actions 3, 9, 28

The Apache web server on this host is an older release with many reported weaknesses. The scanner gives different target lines, so one target must be chosen before work starts. The newer line gives the widest coverage but changes configuration and modules.

Steps in order:

1. Decide the target: the newer 2.4 line, which needs module and configuration testing, or the 2.2 line, which is a smaller change but is also older.
2. Check the site configuration and loaded modules before the change, and note any dependency on older Apache behaviour.
3. Schedule a restart of the web service on TCP port 80 in a change window.
4. Install the chosen Apache release on `metasploitable2.greenbone-community-edition_default` and restart the service.
5. Verify by running the Apache version check and rescanning the Apache checks. Each should no longer report on TCP port 80.

Moving from the 2.2 line to the 2.4 line is a major change. Configuration or module problems can take the site down, so keep a rollback plan.

Band 5 Fix the FTP logins and update ProFTPD

Actions 8, 17, 21, 32

The FTP service on this host sends logins without encryption, and the scanner reported a default-credential finding on it. The ProFTPD release is also old. Changing the login method and the password reduces the risk of logins being captured or guessed. The ProFTPD update removes known weaknesses in the server.

Steps in order:

1. Change the FTP account password that the scanner found with default credentials to a long, unique password. Store it in the approved password vault, not in the ticket.
2. Turn on encrypted FTP by enabling FTPS or enforcing AUTH TLS in the FTP server settings. Disable plain logins once clients are ready.
3. Confirm the installed ProFTPD version. The scanner marks the fix as unresolved, so confirm the release with the ProFTPD project before installing one at or above the stated target.
4. Restart the FTP service in a change window after the changes.
5. Verify by rescanning the FTP checks on TCP port 21 and TCP port 2121 and checking the ProFTPD version.

Moving FTP to encrypted logins may break clients that use plain FTP. Confirm the client list before the change.

Band 5 Check the vsftpd service for compromise, then replace it

Actions 14

The scanner reported a backdoor check against the vsftpd FTP server. The export does not show whether the server was compromised. The compromise check must come before any reinstall, so evidence is kept.

Steps in order:

1. Review the logs, user accounts, running processes and recent file changes on `metasploitable2.greenbone-community-edition_default` for anything unexpected. Do not reinstall yet.
2. If signs of compromise are found, stop further changes and follow your incident process.
3. Obtain a clean vsftpd package from the vendor and verify its signature before installing it.
4. Reinstall vsftpd in a change window and restart the service.
5. Verify by rescanning the vsftpd backdoor check on TCP port 21 and TCP port 6200 and confirming it no longer reports.

The scan cannot show whether this host was compromised. Complete the compromise check before reinstalling.

Band 5 Replace the old jQuery library on the web site

Actions 10, 11

The web site serves old jQuery script files that the scanner reported as having cross-site scripting weaknesses. The fix is a newer library file. It is usually low effort, but a major version change can alter how some pages behave.

Steps in order:

1. Find each copy of jQuery served on TCP port 80 on `metasploitable2.greenbone-community-edition_default`, since the export does not show the file path.
2. Replace each copy with jQuery 3.5.0 or later, which also meets the lower target.
3. Test key pages, forms and menus in a test environment before going live.

4. Verify by rescanning the jQuery checks and checking the file version on the host.

Some pages may depend on behaviour that changed in the newer major version. Test those pages before release.

Band 5 Update Samba file sharing on the host

Actions 12, 30, 36, 40

Samba shares files and printers over the network on TCP port 445. The scanner reported older Samba weaknesses, including local privilege escalation reports. The fixes need a newer release, and the restart interrupts file and print sharing.

Steps in order:

1. Confirm which shares and client machines use this host, since the export does not show them.
2. Upgrade Samba to 3.0.32 or later, and to 3.0.37 or later where the finding title names that release. Check the Samba release notes for the release that fixes the items with no stated version.
3. Schedule a change window, notify users, and restart the Samba services.
4. Verify by checking the Samba version and rescanning the Samba checks on TCP port 445.

Restarting Samba interrupts file and print sharing for users during the change window.

Band 5 Turn off the legacy rlogin service

Actions 13

The rlogin service allows remote logins without encryption and relies on weak trust settings. Turning it off and using SSH instead reduces the exposure of this older login method on the host.

Steps in order:

1. Ask the system owner whether any client or user relies on rlogin. The export does not say.
2. Move any such users to SSH first and confirm they can connect.
3. Disable the rlogin service on TCP port 513 in a change window.
4. Verify by checking that port 513 no longer listens and rescanning the rlogin checks.

Disabling rlogin breaks any client that still depends on it. Confirm the client list before the change.

Band 5 Update the PostgreSQL database on the host

Actions 29, 34, 35

The PostgreSQL database on TCP port 5432 runs an older release with several reported weaknesses. The update needs a database restart, and the applications that use the database must be tested afterwards.

Steps in order:

1. Confirm the installed PostgreSQL release on `metasploitable2.greenbone-community-edition_default`. The scanner gives no target for some items, so confirm the fix with the PostgreSQL vendor's release notes.
2. Choose a supported release and check the upgrade path for the data.
3. Back up the database and test the restore before the change.
4. Schedule a window for the restart and test the applications that use the database afterwards.
5. Verify by checking the server version and rescanning the PostgreSQL checks on TCP port 5432.

A database upgrade needs a planned outage, and applications using this database are unavailable during the restart. The export does not show the support status of the target release.

Band 5 Tighten encryption settings and certificates on the mail and database ports

Actions 15, 16, 18, 19, 20, 22, 23, 24, 25

The services on TCP port 25 and TCP port 5432 use weak encryption settings. The scanner also reported an expired certificate and a weak certificate key. Clients may warn or fail to connect after the change, so the work needs testing before it goes live.

Steps in order:

1. Identify the software on TCP port 25 and TCP port 5432, since the export does not name it.
2. Disable SSLv2, SSLv3, TLSv1.0 and TLSv1.1, and remove the weak cipher suites. Use TLSv1.2 or later.
3. Replace the expired certificate and any certificate with a key shorter than 2048 bits. Reissue any certificate signed with SHA-1 or older hashes using SHA-2.
4. Set the Diffie-Hellman group to 2048 bits or more, or use ECDHE. Disable renegotiation where the software allows it.
5. Restart each service in a change window and test mail and database client connections.
6. Verify by rescanning the TLS and certificate checks on TCP port 25 and TCP port 5432.

Disabling older protocols can stop old clients from connecting. Confirm client versions before the change.

Lower-priority and no-solution items

These items are low or informational, or the scanner gave no solution text for them. They do not block the campaigns above. Items without solution text need a technician to review them manually before any change is planned.

Covered by this review, lower priority:

- Manual review of findings with no solution text on `metasploitable2.greenbone-community-edition_default`, see action 1.
- Low and informational items: 24 actions in total, including the TLS mitigation notes in action 310 and action 325.

- SSH key exchange and weak MAC settings, see action 320 and action 328.
- Samba default configuration notes from the vendor, see action 312.
- ICMP and TCP timestamp settings, see action 324 and action 330.
- Older PHP and Apache items with stated targets, see action 313 and action 326.
- Remaining PEAR and OpenSSH items, see action 331 and action 332.

How findings were prioritised

Each finding is placed in a band. Band 1 holds findings in CISA's Known Exploited Vulnerabilities (KEV) catalog with recorded ransomware use. Band 2 holds findings in that catalog. Band 3 holds a CVE with no catalog match and a CVSS score of 9.0 or higher. Band 4 holds a CVE with no catalog match and a non-trivial rating. Band 5 holds findings with no CVE but a rating of 2 or above. Band 6 holds any other finding.

Bands 1 to 4 hold 0, 0, 0 and 0 findings respectively. Because no CVE identifiers were recorded, the catalog check could not match any finding, so Bands 1 and 2 cannot be ruled in or out for this scan.

The export does not include EPSS exploit prediction scores, so this report does not rely on them.

Actions group findings by fix. Each fix shows the scanner's version target where one is stated. The scanner marks many of those targets as minimums, so a later release may be needed. Bands are applied in order and actions are never moved between bands.

What this scan cannot show

This scan is a point-in-time view from one scanning position. It shows what the scanner could reach and check when it ran. It does not show changes made after that time, or what other network positions can reach. A scan cannot show that a system is free of vulnerabilities.

Other limits in this export:

- Credentials: the export records no failed scanner login for the protocols checked. That does not show the scanner logged in, so credential coverage is unknown. The export does not state whether credentials were used.
- Operating system: 1 of 1 hosts has an operating system fingerprint only, so its operating system was not confirmed by the scan.
- Exploitation status: no CVE identifiers were recorded, so the KEV and ransomware checks could not run. Exploitation status is unknown.
- Fix information: 101 occurrences had no solution text, and several version targets are minimums or unknown.
- Detection confidence: 30 occurrences carry the lowest quality-of-detection rating, so the scanner was less certain of those.
- Severity: 91 occurrences are rated informational by the scanner.
- Scope: only 1 host was in scope. Other systems are not covered by this report.

Appendix: remediation actions

#	Band	Action	Fix target	Systems	Findings	KEV
2	Band 5	Update to version 5.2.15 or later. on 1 system -> eliminates 17 vulnerable instances across 17 findings.	5.2.15	1	17	0
3	Band 5	Update to version 2.4.66 or later. on 1 system -> eliminates 10 vulnerable instances across 10 findings.	2.4.66	1	10	0
4	Band 5	Update to version 5.3.9 or later. on 1 system -> eliminates 9 vulnerable instances across 9 findings.	5.3.9	1	9	0
5	Band 5	Update to version 5.6.31 or later. on 1 system -> eliminates 6 vulnerable instances across 6 findings.	5.6.31	1	6	0
6	Band 5	Update to version 7.2.29 or later. on 1 system -> eliminates 3 vulnerable instances across 3 findings.	7.2.29	1	3	0
7	Band 5	Update to version 4.9.2 or later. on 1 system -> eliminates 3 vulnerable instances across 3 findings.	4.9.2	1	3	0
8	Band 5	Update to version 1.3.2rc3 or later. on 1 system -> eliminates 3 vulnerable instances across 3 findings.	unknown	1	3	0
9	Band 5	Update to version 2.2.22 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.	2.2.22	1	2	0
10	Band 5	Update to version 1.9.0 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.	1.9.0	1	2	0
11	Band 5	Update to version 3.5.0 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.	3.5.0	1	2	0
12	Band 5	Update to version 3.0.32 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.	3.0.32	1	2	0
13	Band 5	Disable the rlogin service and use alternatives like SSH instead. on 1 system -> eliminates 2 vulnerable instances across 2 findings.	unknown	1	2	0
14	Band 5	The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
15	Band 5	The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
16	Band 5	- Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task. - For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
17	Band 5	Change the password as soon as possible. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0

18	Band 5	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
19	Band 5	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
20	Band 5	- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
21	Band 5	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
22	Band 5	Replace the certificate with a stronger key and reissue the certificates it signed. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
23	Band 5	Replace the SSL/TLS certificate by a new one. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
24	Band 5	Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
25	Band 5	Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
26	Band 5	Update to version 2.11.9.5 / 3.1.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
27	Band 5	Update to version 3.1.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
28	Band 5	Update to version 2.2.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.2.9	1	1	0
29	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
30	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
31	Band 5		unknown	1	1	0

		Vendor updates are available. Please see the references for details. on 1 system -> eliminates 1 vulnerable instance across 1 finding.				
32	Band 5	Update to version 1.3.2b, 1.3.3rc2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.2b	1	1	0
33	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
34	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
35	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
36	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
37	Band 5	Update to version 5.2.14, 5.3.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
38	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
39	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
40	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
41	Band 5	Update to version 5.2.14, 5.3.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
42	Band 5	Update to version 3.4.8, 3.5.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
43	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
44	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
45	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
46	Band 5	Updates are available. Please see the references for details. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
47	Band 5	These issues have been fixed in Apache 2.2.16. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
48	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

49	Band 5	Updates are available. Please see the references for details. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
50	Band 5	Vendor updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
51	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
52	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
53	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
54	Band 5	Vendor updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
55	Band 5	Update to version 5.2.17, 5.3.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
56	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
57	Band 5	Updates are available. Please see the references for details. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
58	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
59	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
60	Band 5	Update to version 1.3.3g or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.3g	1	1	0
61	Band 5	Update to version 2.3.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.3.5	1	1	0
62	Band 5	Update to version 5.3.11, 5.4.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
63	Band 5	Change the password as soon as possible. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
64	Band 5	Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
65	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
66	Band 5	Updates are available. Please see the references for details. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

67	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
68	Band 5	Update to version 4.14.14, 4.15.9, 4.16.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
69	Band 5	Update to version 7.4.31, 8.0.24, 8.1.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
70	Band 5	Update to version 4.15.12, 4.16.7, 4.17.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
71	Band 5	Update to version 4.15.13, 4.16.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
72	Band 5	Update to version 4.15.13, 4.16.8, 4.17.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
73	Band 5	Update to version 9.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	9.2	1	1	0
74	Band 5	Update to version 8.0.28, 8.1.16, 8.2.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
75	Band 5	Update to version 9.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	9.3	1	1	0
76	Band 5	Update to version 8.0.22, 8.1.9, 8.2.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
77	Band 5	Update to version 4.16.11, 4.17.10, 4.18.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
78	Band 5	Update to version 4.17.12, 4.18.8, 4.19.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
79	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
80	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
81	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
82	Band 5	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
83	Band 5	Updates are available. Please see the references or vendor advisory for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
84	Band 5	Change the password to something hard to guess or enable password protection at all. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
85	Band 5	Update to version 1.3.6b, 1.3.7rc2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.6b	1	1	0
86	Band 5	Updates are available. Please see the referenced vendor advisory. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

87	Band 5	Updates are available. Please see the referenced vendor advisory. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
88	Band 5	Update to version 3.0.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	3.0.3	1	1	0
89	Band 5	Update to version 5.6.30, 7.0.15, 7.1.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
90	Band 5	Update to version 3.3.10.3, 3.4.3.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
91	Band 5	Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled completely via the 'AllowOverride None' directive within the webserver's configuration. Furthermore all <Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
92	Band 5	Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
93	Band 5	Update to version 7.1.32, 7.3.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
94	Band 5	Update to version 7.1.32 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.1.32	1	1	0
95	Band 5	Update to version 7.2.22, 7.3.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
96	Band 5	Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
97	Band 5	Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
98	Band 5	Update to version 10.6 or 11.1 respectively. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
99	Band 5	Update to version 4.9.5, 5.0.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
100	Band 5	Update to version 4.8.3. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.8.3	1	1	0
101	Band 5	Update to version 1.3.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.7	1	1	0
102	Band 5	Update to version 9.5.25, 9.6.21, 10.16, 11.11, 12.6 or 13.2 respectively. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
103	Band 5	Update to version 8.1.30, 8.2.24, 8.3.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
104	Band 5	Update to version 7.3.29 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.3.29	1	1	0

105	Band 5	Update to version 7.3.31, 7.4.24, 8.0.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
106	Band 5	Update to version 4.13.13, 4.14.9, 4.15.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
107	Band 5	Update to version 4.9.15, 4.10.10, 4.11.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
108	Band 5	Update to version 8.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	8.0	1	1	0
109	Band 5	Update to version 5.4.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	5.4.4	1	1	0
110	Band 5	Update to version 7.0.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.0.12	1	1	0
111	Band 5	Update to version 5.6.29, 7.0.14 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
112	Band 5	Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	9.6	1	1	0
113	Band 5	Update to version 4.17.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.17.1	1	1	0
114	Band 5	Update to version 9.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	9.1	1	1	0
115	Band 5	Update to version 4.8.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.8.6	1	1	0
116	Band 5	Update to version 3.0.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	3.0.0	1	1	0
117	Band 5	Update to version 1.6.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.6.3	1	1	0
118	Band 5	Update to version 6.1.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	6.1.0	1	1	0
119	Band 5	Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
120	Band 5	Update to version 3.4.0 or later. Patch diffs are available for older versions. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	3.4.0	1	1	0
121	Band 5	Update to version 1.3.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.6	1	1	0
122	Band 5	Update to version 1.3.6c or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.6c	1	1	0
123	Band 5	Update to version 4.9.4, 5.0.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
124	Band 5	Update to version 7.2.27, 7.3.14, 7.4.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
125	Band 5	Update to version 9.4.26, 9.5.21, 9.6.17, 10.12, 11.7, 12.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
126	Band 5		unknown	1	1	0

Update to version 7.2.30, 7.3.17, 7.4.5 or later. on 1 system -
> eliminates 1 vulnerable instance across 1 finding.

127	Band 5	Update to version 7.2.31, 7.3.18, 7.4.6 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
128	Band 5	Update to version 7.2.34, 7.3.23, 7.4.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
129	Band 5	Update to version 9.5.23, 9.6.19, 10.14, 11.9, 12.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
130	Band 5	Update to version 4.9.6, 5.0.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
131	Band 5	Update to version 7.3.26, 7.4.14, 8.0.1 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
132	Band 5	Update to version 7.3.27, 7.4.15, 8.0.2 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
133	Band 5	Update to version 7.3.28, 7.4.18 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
134	Band 5	Update to version 7.3.30, 7.4.23, 8.0.10 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
135	Band 5	Update to version 4.14.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.14.8	1	1	0
136	Band 5	Update to version 2.2.32, 2.4.25 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
137	Band 5	Update to version 2.2.27, 2.4.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
138	Band 5	Update to version 2.2.29, 2.4.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
139	Band 5	Update to version 2.2.25, 2.4.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
140	Band 5	Update to version 2.2.25 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.2.25	1	1	0
141	Band 5	Update to version 2.2.24, 2.4.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
142	Band 5	Update to version 2.2.23, 2.4.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
143	Band 5	Update to version 2.2.23, 2.4.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
144	Band 5	Update to version 2.0.65, 2.2.19 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
145	Band 5	Update to version 4.13.14, 4.14.10, 4.15.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
146	Band 5	Update to version 9.6.24, 10.19, 11.14, 12.9, 13.5, 14.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
147	Band 5	Update to version 7.3.33, 7.4.26, 8.0.13 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
148	Band 5		4.15.0	1	1	0

Update to version 4.15.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

149	Band 5	Update to version 4.13.17, 4.14.12, 4.15.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
150	Band 5	Update to version 4.15.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.15.5	1	1	0
151	Band 5	Update to version 7.4.28, 8.0.16, 8.1.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
152	Band 5	Update to version 4.9.10, 5.1.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
153	Band 5	Update to version 7.4.30, 8.0.20, 8.1.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
154	Band 5	Update to version 7.4.33, 8.0.25, 8.1.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
155	Band 5	Update to version 8.0.27, 8.1.14, 8.2.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
156	Band 5	Update to version 8.0.29, 8.1.10, 8.2.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
157	Band 5	Update to version 5.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	5.7	1	1	0
158	Band 5	Update to version 4.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.9	1	1	0
159	Band 5	Apply the patch mentioned in the linked reference. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
160	Band 5	Apply the patch mentioned in the linked reference. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
161	Band 5	Apply the patch mentioned in the linked reference. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
162	Band 5	Update to version 3.4.16, 3.5.14, 3.6.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
163	Band 5	Update to version 3.5.22, 3.6.17, 4.0.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
164	Band 5	Update to version 4.1.22, 4.2.7, 4.3.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
165	Band 5	Update to version 8.1.28, 8.2.18, 8.3.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
166	Band 5	Update to version 8.1.29, 8.2.20, 8.3.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
167	Band 5	Update to version 8.1.31, 8.2.26, 8.3.14 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
168	Band 5	Update to version 13.19, 14.16, 15.11, 16.7, 17.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
169	Band 5	Update to version 8.1.32, 8.2.28 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
170	Band 5		unknown	1	1	0

Update to version 13.21, 14.18, 15.13, 16.9, 17.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

171	Band 5	Update to version 8.1.33, 8.2.29, 8.3.23, 8.4.10 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
172	Band 5	Update to version 13.22, 14.19, 15.14, 16.10, 17.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
173	Band 5	Update to version 1.3.8b or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.8b	1	1	0
174	Band 5	Update to version 1.3.8c or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.8c	1	1	0
175	Band 5	Update to version 1.3.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.9	1	1	0
176	Band 5	Update to version 13.23, 14.20, 15.15, 16.11, 17.7, 18.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
177	Band 5	Update to version 8.2.30, 8.3.29, 8.4.16 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
178	Band 5	Update to version 8.0.30, 8.1.22, 8.2.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
179	Band 5	Update to version 4.2.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.2.4	1	1	0
180	Band 5	Upgrade to version 2.11.9.5 or 3.1.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
181	Band 5	Update to version 5.2.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	5.2.9	1	1	0
182	Band 5	Upgrade to version 4.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.3.1	1	1	0
183	Band 5	Update to version 2.3.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.3.3	1	1	0
184	Band 5	Update to version 2.2.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.2.12	1	1	0
185	Band 5	Update to version 5.2.11, 5.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
186	Band 5	Update to version 5.2.12, 5.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
187	Band 5	Update to version 5.2.14, 5.3.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
188	Band 5	Update to version 5.2.15, 5.3.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
189	Band 5	Update to version 5.2.15, 5.3.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
190	Band 5	Update to version 1.3.3c or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.3c	1	1	0
191	Band 5	- Update to PHP version 5.5.2 or later and set 'session.use_strict_mode' in php.ini to 'On' - make adoptive session with user land code as described in the referenced	unknown	1	1	0

		PHP strict_sessions document on 1 system -> eliminates 1 vulnerable instance across 1 finding.				
192	Band 5	Update to version 5.3.22, 5.4.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
193	Band 5	Update to version 5.3.29, 5.4.24, 5.5.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
194	Band 5	Update to version 5.3.28, 5.4.23, 5.5.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
195	Band 5	Update to version 5.4.32, 5.5.16 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
196	Band 5	Update to version 5.4.29, 5.5.13 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
197	Band 5	- Remove support for 'RSA_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task. - If the service is using OpenSSL: Update to version 0.9.8zd, 1.0.0p, 1.0.1k or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
198	Band 5	Update to PHP version 5.5.21, 5.6.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
199	Band 5	Update to version 5.4.37 or 5.5.21 or 5.6.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
200	Band 5	Update to version 2.4.13 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.4.13	1	1	0
201	Band 5	Update to version 5.4.39, 5.5.23, 5.6.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
202	Band 5	Update to version 5.4.40, 5.5.24, 5.6.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
203	Band 5	Update to version 5.4.40, 5.5.24, 5.6.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
204	Band 5	Update to version 5.4.41, 5.5.25, 5.6.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
205	Band 5	Update to version 5.4.38, 5.5.22, 5.6.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
206	Band 5	Update to version 5.5.24, 5.6.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
207	Band 5	Update to version 9.0.20, 9.1.16, 9.2.11, 9.3.7, 9.4.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
208	Band 5	Update to version 5.5.30, 5.6.14 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
209	Band 5	Update to version 5.4.44, 5.5.28, 5.6.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
210	Band 5	Update to version 5.5.31, 5.6.17, 7.0.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
211	Band 5	Update to version 5.4.45, 5.5.29, 5.6.13 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

212	Band 5	Update to version 5.4.43, 5.5.27, 5.6.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
213	Band 5	Upgrade to version 9.1.20 or 9.2.15 or 9.3.11 or 9.4.6 or 9.5.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
214	Band 5	Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
215	Band 5	Update to PHP version 5.5.33, 5.6.19 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
216	Band 5	Update to version 5.5.34, 5.6.20, 7.0.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
217	Band 5	Update to version 5.5.35, 5.6.21, 7.0.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
218	Band 5	Update to version 5.4.44, 5.5.28, 5.6.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
219	Band 5	Update to version 5.5.32, 5.6.18, 7.0.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
220	Band 5	Update to version 5.6.18, 7.0.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
221	Band 5	Update to version 5.5.28, 5.6.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
222	Band 5	Update to PHP version 5.5.22, 5.6.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
223	Band 5	Update to version 5.4.45, 5.5.29, 5.6.13 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
224	Band 5	Update to version 5.6.24, 7.0.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
225	Band 5	Update to version 2.4.24, or 2.2.32, or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
226	Band 5	Update to version 5.5.38, 5.6.24, 7.0.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
227	Band 5	Upgrade to version 9.1.23 or 9.2.18 or 9.3.14 or 9.4.9 or 9.5.4 or higher. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
228	Band 5	Update to version 5.4.44, 5.5.28, 5.6.12, 7.0.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
229	Band 5	Update to version 5.5.27, 5.6.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
230	Band 5	Update to version 5.4.42, 5.5.26, 5.6.10 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
231	Band 5	Update to PHP version 5.5.37, 5.6.23, 7.0.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
232	Band 5	Update to version 5.5.37, 5.6.23 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
233	Band 5	Update to version 5.5.36, 5.6.22 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

234	Band 5	Update to version 5.5.36, 5.6.22, 7.0.7 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
235	Band 5	Update to version 5.4.38, 5.5.22, 5.6.6 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
236	Band 5	Update to version 5.5.31, 5.6.17, 7.0.2 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
237	Band 5	Update to version 7.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.3	1	1	0
238	Band 5	Update to version 5.6.26, 7.0.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
239	Band 5	Update to version 5.6.25, 7.0.10 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
240	Band 5	Update to version 5.6.27, 7.0.12 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
241	Band 5	Update to version 7.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.4	1	1	0
242	Band 5	Update to version 1.3.5e, 1.3.6rc5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.3.5e	1	1	0
243	Band 5	Update to version 7.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.2	1	1	0
244	Band 5	Update to version 5.6.31, 7.0.21, 7.1.7 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
245	Band 5	Update to version 5.6.31, 7.0.17, 7.1.3 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
246	Band 5	Update to version 5.6.28, 7.0.13 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
247	Band 5	Upgrade to Samba 4.6.8, 4.5.14 and 4.4.16 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
248	Band 5	Update to version 7.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.6	1	1	0
249	Band 5	Update to version 5.6.32, 7.0.25, 7.1.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
250	Band 5	Update to version 5.5.32, 5.6.18, 7.0.3 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
251	Band 5	Update to version 7.1.20, 7.2.8, 7.3.0alpha3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
252	Band 5	Update to version 5.6.33, 7.0.27, 7.1.13, 7.2.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
253	Band 5	Update to version 5.6.34, 7.0.28, 7.1.15, 7.2.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
254	Band 5	Update to version 5.6.36, 7.0.30, 7.1.17, 7.2.5 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
255	Band 5	Update to version 5.6.35, 7.0.29, 7.1.16, 7.2.4 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
256	Band 5		4.8.2	1	1	0

Upgrade to version 4.8.2 or newer. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

257	Band 5	Update to version 7.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.8	1	1	0
258	Band 5	Update to version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
259	Band 5	Fixed is available in the SVN repository, please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
260	Band 5	Upgrade to respective version below, PostgreSQL 8.3.7 or 8.2.13 or 8.1.17 or 8.0.21 or 7.4.25. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
261	Band 5	Update to version 3.3.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	3.3.6	1	1	0
262	Band 5	Update to Apache HTTP Server version 2.0.64, 2.2.14 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
263	Band 5	- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
264	Band 5	- Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later - For other products using Tomcat please contact the vendor for more information on fixed versions on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
265	Band 5	A whole cleanup of the infected system is recommended. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
266	Band 5	Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting \$SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
267	Band 5	All Samba users should upgrade to the latest version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
268	Band 5	As a workaround disable mod_copy in the ProFTPD configuration file. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
269	Band 5	Delete the listed files or restrict access to them. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
270			unknown	1	1	0

	Band 5	Disable class-loading. Please contact the vendor of the affected system for additional guidance. on 1 system -> eliminates 1 vulnerable instance across 1 finding.				
271	Band 5	Disable the reported weak encryption algorithm(s). on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
272	Band 5	Disable the reported weak host key algorithm(s). on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
273	Band 5	Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
274	Band 5	Disable the rexec service and use alternatives like SSH instead. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
275	Band 5	Disable the rsh service and use alternatives like SSH instead. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
276	Band 5	Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
277	Band 5	Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
278	Band 5	If not needed disable the directory listing/indexing within the web servers config. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
279	Band 5	If you do not want to share files, you should disable anonymous logins. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
280	Band 5	PHP: Update to version 5.3.13, 5.4.3 or later - Other products / applications: Please contact the vendor for a solution on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
281	Band 5	Replace Telnet with a protocol like SSH which supports encrypted connections. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
282	Band 5	Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
283	Band 5	Update jQuery on the remote host to a still supported version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
284	Band 5		unknown	1	1	0

Update the Apache HTTP Server version on the remote host to a still supported version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

285	Band 5	Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor. Note / Important: Please create an override for this result if the target host is a: - Windows system with Extended Security Updates (ESU) - System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
286	Band 5	Update the PHP version on the remote host to a still supported version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
287	Band 5	Update the phpMyAdmin version on the remote host to a still supported version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
288	Band 5	Update the PostgreSQL version on the remote host to a still supported version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
289	Band 5	Update the Samba version on the remote host to a still supported version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
290	Band 5	Update to Apache HTTP Server 2.2.32 or 2.4.25 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
291	Band 5	Update to Apache HTTP Server 2.2.33 or 2.4.26 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
292	Band 5	Update to Apache HTTP Server 2.2.34 or 2.4.27 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
293	Band 5	Update to PHP 5.2.15 or 5.3.4 on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
294	Band 5	Update to version 7.1p2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
295	Band 5	Update to version 7.2p2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
296	Band 5	Update to version 7.2p2-3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
297	Band 5	Update to version 9.3p2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
298	Band 5	Updates are available. Update to newer Version. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
299	Band 5	Upgrade to phpMyAdmin version 3.2.0.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
300	Band 5	Upgrade to PostgreSQL version 9.2.21 or 9.3.17 or 9.4.12 or 9.5.7 or 9.6.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
301	Band 5	Upgrade to Samba 4.4.10 or 4.5.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
302	Band 5	Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <Directory /	unknown	1	1	0

usr/doc> AllowOverride None order deny, allow deny from all
allow from localhost </Directory> on 1 system -> eliminates
1 vulnerable instance across 1 finding.

303	Band 5	Use access restrictions to these dangerous HTTP methods or disable them completely. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
304	Band 5	Vendor updates are available. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
305	Band 5	Update to Apache HTTP Server version 2.2.22 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.2.22	1	1	0
306	Band 5	Upgrade to OpenSSH version 6.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	6.9	1	1	0
307	Band 5	Upgrade to OpenSSH 7.0 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	7.0	1	1	0
308	Band 5	Upgrade to phpMyAdmin version 3.3.7 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	3.3.7	1	1	0
309	Band 5	Upgrade to TWiki version 4.3.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.3.2	1	1	0
1	Band 5	Manually review 79 findings on 1 system — the scan supplied no solution text; 100 vulnerable instances remain open.	unknown	1	79	0
310	Band 6	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+ on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
311	Band 6	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
312	Band 6	The vendor commented on the issue stating that it stems from an insecure default configuration. The Samba team advises administrators to set 'wide links = no' in the '[global]' section of 'smb.conf' and then restart the service to correct misconfigured services. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
313	Band 6	Update to version 3.5.11 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	3.5.11	1	1	0
314	Band 6	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
315	Band 6	Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
316	Band 6	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
317	Band 6	Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

318	Band 6	Update to version 4.13.16 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	4.13.16	1	1	0
319	Band 6	Update to version 10.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	10.1	1	1	0
320	Band 6	Update the remote SSH server to a version supporting PQC KEX algorithms (e.g. OpenSSH 8.9 or later) and enable relevant PQC KEX algorithms accordingly. Please see the references/manual of the remote SSH server and/or contact the vendor of it for more support. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
321	Band 6	Update to version 7.2.33, 7.3.21, 7.4.9 or later. on 1 system - > eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
322	Band 6	Update to version 5.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	5.1	1	1	0
323	Band 6	Update to version 4.4.5, 5.1.7, 5.2.6 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
324	Band 6	To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
325	Band 6	- Remove support for 'DHE_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task. - If the service is using OpenSSL: Update to version 1.0.1n, 1.0.2b or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
326	Band 6	Update to Apache HTTP Server version 2.0.64, 2.2.14 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
327	Band 6	Apply the patch linked in the references. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
328	Band 6	Disable the reported weak MAC algorithm(s). on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
329	Band 6	Update to the most recent version of Apache HTTP Server. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
330	Band 6	Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks) on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
331	Band 6	Update to a later PHP version including an PEAR installer in version 1.9.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.9.2	1	1	0

332	Band 6	Upgrade to OpenSSH 5.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	5.2	1	1	0
-----	---------------	--	-----	---	---	---

Technical detail by action

2. Update to version 5.2.15 or later. on 1 system -> eliminates 17 vulnerable instances across 17 findings.

Band 5

Findings	PHP <= 5.2.8 Multiple Vulnerabilities; PHP < 5.2.12 Multiple Vulnerabilities; PHP < 5.2.13 Multiple Vulnerabilities; PHP < 5.2.10 JPEG Image Processing DoS Vulnerability; PHP < 5.2.14 Multiple Vulnerabilities; PHP < 5.2.5 Multiple Vulnerabilities; PHP < 5.2.6 Multiple Vulnerabilities; PHP < 5.2.7 Multiple Vulnerabilities; PHP < 5.2.6 Multiple Vulnerabilities (Aug 2008); PHP < 5.2.8 XSS Vulnerability; PHP < 5.2.15 Security Bypass Vulnerability; PHP 5.2.x < 5.2.7 Buffer Overflow Vulnerability (Jan 2015); PHP Security Bypass and File Writing Vulnerabilities (Dec 2008); PHP 4.3.x < 5.2.7 Buffer Overflow Vulnerability; PHP 5.x < 5.2.9 Memory Information Disclosure Vulnerability; PHP Multiple Vulnerabilities (Sep 2009); PHP 4.x, 5.2.6 DoS Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('5.2.4', 1)
Fix target	5.2.15
Fixed version	PHP 5.2.15
Scanner plugins	1.3.6.1.4.1.25623.1.0.100146, 1.3.6.1.4.1.25623.1.0.100409, 1.3.6.1.4.1.25623.1.0.100511, 1.3.6.1.4.1.25623.1.0.100581, 1.3.6.1.4.1.25623.1.0.108861, 1.3.6.1.4.1.25623.1.0.108866, 1.3.6.1.4.1.25623.1.0.108867, 1.3.6.1.4.1.25623.1.0.108868, 1.3.6.1.4.1.25623.1.0.800110, 1.3.6.1.4.1.25623.1.0.800334, 1.3.6.1.4.1.25623.1.0.801731, 1.3.6.1.4.1.25623.1.0.805410, 1.3.6.1.4.1.25623.1.0.900184, 1.3.6.1.4.1.25623.1.0.900185, 1.3.6.1.4.1.25623.1.0.900186, 1.3.6.1.4.1.25623.1.0.900871, 1.3.6.1.4.1.25623.1.0.900925

3. Update to version 2.4.66 or later. on 1 system -> eliminates 10 vulnerable instances across 10 findings.

Band 5

Findings	Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux; Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux; Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux; Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux; Apache HTTP Server < 2.4.66 SSI Vulnerability - Linux; Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux; Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux; Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux; Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux; Apache HTTP Server < 2.4.64 Multiple Vulnerabilities - Linux
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('2.2.8', 1)
Fix target	2.4.66
Fixed version	Apache HTTP Server 2.4.66
Scanner plugins	1.3.6.1.4.1.25623.1.0.100272, 1.3.6.1.4.1.25623.1.0.113837, 1.3.6.1.4.1.25623.1.0.114682, 1.3.6.1.4.1.25623.1.0.117856, 1.3.6.1.4.1.25623.1.0.125564, 1.3.6.1.4.1.25623.1.0.146725, 1.3.6.1.4.1.25623.1.0.148252, 1.3.6.1.4.1.25623.1.0.149152, 1.3.6.1.4.1.25623.1.0.152039, 1.3.6.1.4.1.25623.1.0.154909

4. Update to version 5.3.9 or later. on 1 system -> eliminates 9 vulnerable instances across 9 findings. **Band 5**

Findings	PHP 5.x < 5.3.3 Information Disclosure Vulnerability; PHP 5.x < 5.3.4 Improper Input Validation Vulnerability; PHP < 5.3.6 Remote Integer Overflow Vulnerability; PHP 5.3.x < 5.3.7 Multiple Security Vulnerabilities; PHP 5.x < 5.3.9 Security Bypass Vulnerability; PHP < 5.3.3 Multiple Vulnerabilities; PHP < 5.3.4 Multiple Vulnerabilities; PHP < 5.3.4 Multiple Security Bypass Vulnerabilities; PHP < 5.3.7 Use After Free Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('5.2.4', 1)
Fix target	5.3.9
Fixed version	PHP 5.3.9
Scanner plugins	1.3.6.1.4.1.25623.1.0.100695, 1.3.6.1.4.1.25623.1.0.100901, 1.3.6.1.4.1.25623.1.0.103113, 1.3.6.1.4.1.25623.1.0.103229, 1.3.6.1.4.1.25623.1.0.103464, 1.3.6.1.4.1.25623.1.0.108869, 1.3.6.1.4.1.25623.1.0.108870, 1.3.6.1.4.1.25623.1.0.801585, 1.3.6.1.4.1.25623.1.0.902356

5. Update to version 5.6.31 or later. on 1 system -> eliminates 6 vulnerable instances across 6 findings.

Band 5

Findings	PHP < 5.6.5 Multiple Vulnerabilities (Jan 2015); PHP < 5.6.12 Multiple DoS Vulnerabilities - Linux; PHP < 5.6.0 DoS Vulnerability - Linux; PHP < 5.6.7 DoS Vulnerability - Linux; PHP < 5.6.26 DoS Vulnerability - Linux; PHP < 5.6.31 DoS Vulnerability - Linux
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('5.2.4', 1)
Fix target	5.6.31
Fixed version	PHP 5.6.31
Scanner plugins	1.3.6.1.4.1.25623.1.0.805413, 1.3.6.1.4.1.25623.1.0.808611, 1.3.6.1.4.1.25623.1.0.808669, 1.3.6.1.4.1.25623.1.0.808673, 1.3.6.1.4.1.25623.1.0.809321, 1.3.6.1.4.1.25623.1.0.811490

6. Update to version 7.2.29 or later. on 1 system -> eliminates 3 vulnerable instances across 3 findings.

Band 5

Findings	PHP < 7.2.26 Multiple Vulnerabilities (Dec 2019) - Linux; PHP < 7.2.28 Multiple Vulnerabilities (Feb 2020) - Linux; PHP < 7.2.29 Multiple Vulnerabilities (Mar 2020) - Linux
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('5.2.4', 1)
Fix target	7.2.29
Fixed version	PHP 7.2.29
Scanner plugins	1.3.6.1.4.1.25623.1.0.143276, 1.3.6.1.4.1.25623.1.0.143541, 1.3.6.1.4.1.25623.1.0.143615

7. Update to version 4.9.2 or later. on 1 system -> eliminates 3 vulnerable instances across 3 findings. **Band 5**

Findings	phpMyAdmin < 4.9.0 CSRF Vulnerability (PMASA-2019-4) - Linux; phpMyAdmin < 4.9.1 CSRF Vulnerability - Linux; phpMyAdmin < 4.9.2 Multiple Vulnerabilities (PMASA-2019-5) - Linux
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('3.1.1', 1)
Fix target	4.9.2
Fixed version	phpMyAdmin 4.9.2
Scanner plugins	1.3.6.1.4.1.25623.1.0.142499, 1.3.6.1.4.1.25623.1.0.142897, 1.3.6.1.4.1.25623.1.0.143167

8. Update to version 1.3.2rc3 or later. on 1 system -> eliminates 3 vulnerable instances across 3 findings.

Band 5

Findings	ProFTPD < 1.3.2rc3 DoS Vulnerability; ProFTPD < 1.3.2rc3 CSRF Vulnerability; ProFTPD 1.3.1 - 1.3.2rc2 SQLi Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Installed	('1.3.1', 1)
Fixed version	ProFTPD 1.3.2rc3
Scanner plugins	1.3.6.1.4.1.25623.1.0.801640, 1.3.6.1.4.1.25623.1.0.900133, 1.3.6.1.4.1.25623.1.0.900507

9. Update to version 2.2.22 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.

Band 5

Findings	Apache HTTP Server Multiple Security Vulnerabilities; Apache HTTP Server Multiple Vulnerabilities (Jan 2012) - Linux
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('2.2.8', 1)
Fix target	2.2.22
Fixed version	Apache HTTP Server 2.2.22
Scanner plugins	1.3.6.1.4.1.25623.1.0.100514, 1.3.6.1.4.1.25623.1.0.147057

10. Update to version 1.9.0 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.

Band 5

Findings	jQuery < 1.9.0 XSS Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('1.3.2', 1)
Fix target	1.9.0
Fixed version	jQuery 1.9.0
Scanner plugins	1.3.6.1.4.1.25623.1.0.141636, 1.3.6.1.4.1.25623.1.0.143968

11. Update to version 3.5.0 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.

Band 5

Findings	jQuery 1.2 < 3.5.0 XSS Vulnerability; jQuery 1.0.3 < 3.5.0 XSS Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('1.3.2', 1)
Fix target	3.5.0
Fixed version	jQuery 3.5.0
Scanner plugins	1.3.6.1.4.1.25623.1.0.143812, 1.3.6.1.4.1.25623.1.0.143813

12. Update to version 3.0.32 or later. on 1 system -> eliminates 2 vulnerable instances across 2 findings.

Band 5

Findings	Samba 3.0.6 <= 3.0.23d Multiple Vulnerabilities; Samba < 3.0.32 winbind Daemon DoS Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 445
Installed	('3.0.20', 1)
Fix target	3.0.32
Fixed version	Samba 3.0.32
Scanner plugins	1.3.6.1.4.1.25623.1.0.150723, 1.3.6.1.4.1.25623.1.0.800711

13. Disable the rlogin service and use alternatives like SSH instead. on 1 system -> eliminates 2 vulnerable instances across 2 findings. Band 5

Findings rlogin Passwordless Login; The rlogin service is running
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 513
Scanner plugins 1.3.6.1.4.1.25623.1.0.113766, 1.3.6.1.4.1.25623.1.0.901202

14. The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 21, TCP port 6200
Scanner plugins 1.3.6.1.4.1.25623.1.0.103185

15. The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings SSL/TLS: Report Weak Cipher Suites
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 25, TCP port 5432
Scanner plugins 1.3.6.1.4.1.25623.1.0.103440

16. - Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task. - For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 25, TCP port 5432
Scanner plugins 1.3.6.1.4.1.25623.1.0.106223

17. Change the password as soon as possible. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings FTP Brute Force Logins With Default Credentials Reporting
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 21, TCP port 2121
Scanner plugins 1.3.6.1.4.1.25623.1.0.108718

18. It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 25, TCP port 5432
Scanner plugins 1.3.6.1.4.1.25623.1.0.111012

19. It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 25, TCP port 5432
Scanner plugins 1.3.6.1.4.1.25623.1.0.117274

20. - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities. on 1 system -> eliminates 2 vulnerable instances across 1 finding.

Band 5

Findings	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 25, TCP port 5432
Scanner plugins	1.3.6.1.4.1.25623.1.0.117840

21. Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information. on 1 system -> eliminates 2 vulnerable instances across 1 finding.

Band 5

Findings	FTP Unencrypted Cleartext Login
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 21, TCP port 2121
Scanner plugins	1.3.6.1.4.1.25623.1.0.108528

22. Replace the certificate with a stronger key and reissue the certificates it signed. on 1 system -> eliminates 2 vulnerable instances across 1 finding.

Band 5

Findings	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 25, TCP port 5432
Scanner plugins	1.3.6.1.4.1.25623.1.0.150710

23. Replace the SSL/TLS certificate by a new one. on 1 system -> eliminates 2 vulnerable instances across 1 finding.

Band 5

Findings	SSL/TLS: Certificate Expired
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 25, TCP port 5432
Scanner plugins	1.3.6.1.4.1.25623.1.0.103955

24. Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings. on 1 system -> eliminates 2 vulnerable instances across 1 finding.

Band 5

Findings	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 25, TCP port 5432
Scanner plugins	1.3.6.1.4.1.25623.1.0.105880

25. Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service. on 1 system -> eliminates 2 vulnerable instances across 1 finding.

Band 5

Findings	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 25, TCP port 5432
Scanner plugins	1.3.6.1.4.1.25623.1.0.117761

26. Update to version 2.11.9.5 / 3.1.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings phpMyAdmin Code Injection and XSS Vulnerability
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('3.1.1', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100077

27. Update to version 3.1.3.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('3.1.1', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100078

28. Update to version 2.2.9 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings Apache HTTP Server 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('2.2.8', 1)
Fix target 2.2.9
Scanner plugins 1.3.6.1.4.1.25623.1.0.100211

29. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings PostgreSQL Multiple Security Vulnerabilities (Sep 2009)
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 5432
Installed ('8.3.1', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100273

30. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings Samba < 3.0.37, 3.1.x < 3.2.15, 3.3.x < 3.3.8, 3.4.x < 3.4.2 Multiple Vulnerabilities
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 445
Installed ('3.0.20', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100306

31. Vendor updates are available. Please see the references for details. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('3.1.1', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100307

32. Update to version 1.3.2b, 1.3.3rc2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

Band 5

Findings	ProFTPD < 1.3.2b, 1.3.3 - 1.3.3.rc1 SSL Certificate Validation Bypass Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Installed	('1.3.1', 1)
Fix target	1.3.2b
Scanner plugins	1.3.6.1.4.1.25623.1.0.100316

33. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. **Band 5**

Findings	PHP < 5.3.1 Multiple Vulnerabilities
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('5.2.4', 1)
Scanner plugins	1.3.6.1.4.1.25623.1.0.100359

34. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. **Band 5**

Findings	PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 5432
Installed	('8.3.1', 1)
Scanner plugins	1.3.6.1.4.1.25623.1.0.100400

35. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. **Band 5**

Findings	PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 5432
Installed	('8.3.1', 1)
Scanner plugins	1.3.6.1.4.1.25623.1.0.100470

36. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. **Band 5**

Findings	Samba <= 3.4.5 'mount.cifs' Utility Local Privilege Escalation Vulnerability
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 445
Installed	('3.0.20', 1)
Scanner plugins	1.3.6.1.4.1.25623.1.0.100476

37. Update to version 5.2.14, 5.3.3 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

Band 5

Findings	PHP 5.3.1 Multiple DoS Vulnerabilities
Systems	metasploitable2.greenbone-community-edition_default
Services	TCP port 80
Installed	('5.2.4', 1)
Scanner plugins	1.3.6.1.4.1.25623.1.0.100529

38. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings PHP 4.4.x < 4.4.9, 5.2.x < 5.2.8 DoS Vulnerability
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('5.2.4', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100582

39. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings PHP Multiple Buffer Overflow Vulnerabilities
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('5.2.4', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100583

40. Updates are available. Please see the references for more information. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerability
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 445
Installed ('3.0.20', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100623

41. Update to version 5.2.14, 5.3.2 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 5

Findings PHP 5.2.x < 5.2.14, 5.3.x < 5.3.3 Multiple RCE Vulnerabilities
Systems metasploitable2.greenbone-community-edition_default
Services TCP port 80
Installed ('5.2.4', 1)
Scanner plugins 1.3.6.1.4.1.25623.1.0.100631

Data sources & licensing

This report uses public data from the sources below. It was extracted and normalized for this report; no source endorses this report. The attribution each source's licence or terms ask for is printed with the source it belongs to.

KEV catalog (Required feed)

Data used: retrieved 2026-10-18.

The KEV database is distributed under the Creative Commons 0 1.0 License (<https://creativecommons.org/publicdomain/zero/1.0/>). Use of the information does not authorize use of the CISA Logo or DHS Seal, nor should such use be interpreted as an endorsement by CISA or DHS.

Source: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

EPSS (Required feed)

EPSS scores: Exploit Prediction Scoring System (EPSS), FIRST, <https://www.first.org/epss/>, score date 2026-10-18.

The words in this report were written by an AI model (claude-haiku-5-5) and checked automatically before release. Every count, priority band and KEV status comes from the scoring engine, not the model. Validate changes before applying them. Rules 7ee05e85a8d6.