



CVE-2021-29504

Published on: 06/07/2021 12:00:00 AM UTC

Last Modified on: 06/17/2021 03:33:00 PM UTC

CVE-2021-29504 - advisory for GHSA-rwgm-f83r-v3qj

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Wp-cli](#) from [Wp-cli](#) contain the following vulnerability:

WP-CLI is the command-line interface for WordPress. An improper error handling in HTTPS requests management in WP-CLI version 0.12.0 and later allows remote attackers able to intercept the communication to remotely disable the certificate verification on WP-CLI side, gaining full control over the communication content, including

the ability to impersonate update servers and push malicious updates towards WordPress instances controlled by the vulnerable WP-CLI agent, or push malicious updates toward WP-CLI itself. The vulnerability stems from the fact that the default behavior of ``WP_CLI\Utils\http_request()`` when encountering a TLS handshake error is to disable certificate validation and retry the same request. The default behavior has been changed with version 2.5.0 of WP-CLI and the ``wp-cli/wp-cli`` framework (via <https://github.com/wp-cli/wp-cli/pull/5523>) so that the ``WP_CLI\Utils\http_request()`` method accepts an ``$insecure`` option that is ``false`` by default and consequently that a TLS handshake failure is a hard error by default. This new default is a breaking change and ripples through to all consumers of ``WP_CLI\Utils\http_request()``, including those in separate WP-CLI bundled or third-party packages. <https://github.com/wp-cli/wp-cli/pull/5523> has also added an ``--insecure`` flag to the ``cli update`` command to counter this breaking change. There is no direct workaround for the default insecure behavior of ``wp-cli/wp-cli`` versions before 2.5.0. The workaround for dealing with the breaking change in the commands directly affected by the new secure default behavior is to add the ``--insecure`` flag to manually opt-in to the previous insecure behavior.

CVE-2021-29504 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **wp-cli** - **wp-cli** version < 2.5.0

CVSS3 Score: **7.4 - HIGH**

Attack
Vector

NETWORK

Attack
Complexity

HIGH

Privileges
Required

NONE

User
Interaction

NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE
CVSS2 Score: 7.5 - HIGH			
Access Vector	Access Complexity	Authentication	
NETWORK	LOW	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	PARTIAL	PARTIAL	

CVE References

Description	Tags	Link
Add <code>--insecure</code> flag to <code>core download</code> & <code>core update</code> commands by schlessera · Pull Request #186 · wp-cli/core-command · GitHub	github.com text/html	 MISC github.com/wp-cli/core-command/pull/186
Add <code>--insecure</code> flag to <code>package install</code> command by schlessera · Pull Request #138 · wp-cli/package-command · GitHub	github.com text/html	 MISC github.com/wp-cli/package-command/pull/138
Disable automatic retry by default on certificate validation error by schlessera · Pull Request #5523 · wp-cli/wp-cli · GitHub	github.com text/html	 MISC github.com/wp-cli/wp-cli/pull/5523
Add <code>--insecure</code> flag to <code>core plugin verify-checksums</code> commands by schlessera · Pull Request #86 · wp-cli/checksum-command · GitHub	github.com text/html	 MISC github.com/wp-cli/checksum-command/pull/86
Improper Certificate Validation in WP-CLI framework · Advisory · wp-cli/wp-cli · GitHub	github.com text/html	 CONFIRM github.com/wp-cli/security/advisories/GHSA-rwgm-f83r-v3qj
Add <code>--insecure</code> flag to <code>config create</code> & <code>config shuffle-salts</code> commands by schlessera · Pull Request #128 · wp-cli/config-command · GitHub	github.com text/html	 MISC github.com/wp-cli/config-command/pull/128
Add <code>--insecure</code> flag to <code>plugin theme install</code> & <code>plugin theme update</code> commands by schlessera · Pull Request #287 · wp-cli/extension-command · GitHub	github.com text/html	 MISC github.com/wp-cli/extension-command/pull/287

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-cli	Wp-cli	All	All	All	All
cpe:2.3:a:wp-cli:wp-cli:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-29504 : WP-CLI is the command-line interface for WordPress. An improper error handling in HTTPS requests m... twitter.com/i/web/status/1...	2021-06-07 20:54:13
 /r/netcve	CVE-2021-29504	2021-06-07 21:41:53

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)