

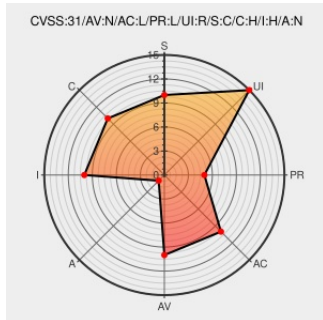


CVE-2020-26222

Published on: 11/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26222 - advisory for GHSA-23f7-99jx-m54r

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

Certain versions of [Dependabot](#) from [Dependabot Project](#) contain the following vulnerability:

Dependabot is a set of packages for automated dependency management for Ruby, JavaScript, Python, PHP, Elixir, Rust, Java, .NET, Elm and Go. In Dependabot-Core from version 0.119.0.beta1 before version 0.125.1, there is a remote code execution vulnerability in dependabot-common and dependabot-go_modules when a source

branch name contains malicious injectable bash code. For example, if Dependabot is configured to use the following source branch name: `"/${curl,127.0.0.1}"`, Dependabot will make a HTTP request to the following URL: 127.0.0.1 when cloning the source repository. The fix was applied to version 0.125.1. As a workaround, one can escape the branch name prior to passing it to the Dependabot::Source class.

CVE-2020-26222 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [dependabot](#) - **dependabot-core** version < 0.125.1

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
v0.125.1 by feelepxyz · Pull Request #2727 · dependabot/dependabot-core · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/dependabot/dependabot-core/pull/2727
Remote code execution in dependabot-core branch names when cloning · Advisory · dependabot/dependabot-core · GitHub	Exploit Third Party Advisory github.com text/html	 CONFIRM github.com/dependabot/dependabot-core/security/advisories/GHSA-23f7-99jx-m54r
Merge pull request #2727 from dependabot/v0.125.1-release-notes · dependabot/dependabot-core@e089116 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/dependabot/dependabot-core/commit/e089116abbe284425b976f7920e502b8e83a61b5

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	Dependabot Project	Dependabot	All	All	All	All
Application	Dependabot Project	Dependabot	0.119.0	-	All	All
Application	Dependabot Project	Dependabot	0.119.0	beta1	All	All
Application	Dependabot Project	Dependabot	All	All	All	All
Application	Dependabot Project	Dependabot	0.119.0	-	All	All
Application	Dependabot Project	Dependabot	0.119.0	beta1	All	All

cpe:2.3:a:dependabot_project:dependabot:*****:.*:

cpe:2.3:a:dependabot_project:dependabot:0.119.0:-:*****:.*:

cpe:2.3:a:dependabot_project:dependabot:0.119.0:beta1:*****:.*:

cpe:2.3:a:dependabot_project:dependabot:*****:.*:

cpe:2.3:a:dependabot_project:dependabot:0.119.0:-:*****:.*:

cpe:2.3:a:dependabot_project:dependabot:0.119.0:beta1:*****:.*:

No vendor comments have been submitted for this CVE

© [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](#)