



CVE-2022-24433

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-24433
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-11 17:16:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	The package simple-git before 3.3.0 are vulnerable to Command Injection via argument injection. When calling the .fetch(re

Risk And Classification

Problem Types: CWE-88

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple-git Project	Simple-git	All	All	All	All

References

Reference	Source
Prevent use of `--upload-pack` as a command in `git.fetch` to avoid p... by steveukx · Pull Request #767 · steveukx/git-js · GitHub	MISC
Command Injection in org.webjars.npm:simple-git CVE-2022-24433 Snyk	MISC
Command Injection in simple-git CVE-2022-24433 Snyk	MISC
Release simple-git@3.3.0 · steveukx/git-js · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Alessio Della Libera of Snyk Research Team

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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