



simple-git has blockUnsafeOperationsPlugin bypass via case-insensitive protocol.allow config key that enables RCE

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

Summary

CVE	CVE-2026-28292
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 19:17:20 UTC
Updated	2026-04-14 16:16:38 UTC
Description	`simple-git`, an interface for running git commands in any node.js application, has an issue in versions 3.15.0 through 3.32.0 that allows an attacker to bypass the blockUnsafeOperationsPlugin via a case-insensitive protocol.allow config key that enables RCE.

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security-advisories@github.com

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.001030000 probability, percentile 0.281920000 (date 2026-04-15)

Problem Types: CWE-78 | CWE-178 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-178 CWE-178: Improper Handling of Case Sensitivity

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Score

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Steveuxx	Simple-git	affected >= 3.15.0, < 3.32.3	Not specified

References

Reference	Source	Link
github.com/steveuxx/git-js/commit/f7042088aa2dac59e3c49a84d7a2f4b26048a257	security-advisories@github.com	github.com
www.codeant.ai/security-research/security-research-simple-git-remote-code-ex...	security-advisories@github.com	www.codeant.ai
www.codeant.ai/security-research/simple-git-remote-code-execution-cve-2026-2...	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.codeant.ai
github.com/steveuxx/git-js/security/advisories/GHSA-r275-fr43-pm7q	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

