



# CVE-2026-6951

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

## Summary

<b>CVE</b>	CVE-2026-6951
<b>State</b>	PUBLISHED
<b>Assigner</b>	snyk
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-25 06:16:16 UTC
<b>Updated</b>	2026-04-25 11:16:17 UTC
<b>Description</b>	Versions of the package simple-git before 3.36.0 are vulnerable to Remote Code Execution (RCE) due to an incomplete fix

## Risk And Classification

**Primary CVSS:** v4.0 9.2 CRITICAL from report@snyk.io

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-94 | CWE-94 Remote Code Execution (RCE)

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/C
4.0	CNA	DECLARED	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P
3.1	report@snyk.io	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/E:P

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Simple-git	affected 3.36.0 semver	Not specified

### References

Reference	Source	Link
security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-15456078	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="#">security.snyk.io</a>
github.com/steveukx/git-js/commit/89a2294febed5dfe737c4c735d936bb6018746a8	report@snyk.io	<a href="#">github.com</a>

<a href="https://gist.github.com/KKC73/02d1d97f3410756095b501fda0ac8ca6">gist.github.com/KKC73/02d1d97f3410756095b501fda0ac8ca6</a>	<a href="mailto:report@snyk.io">report@snyk.io</a>	<a href="https://gist.github.com">gist.github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Kuycheu Kung (en)

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)