



CVE-2020-15123

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

Summary

CVE	CVE-2020-15123
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-20 18:15:00 UTC
Updated	2020-07-27 19:00:00 UTC
Description	In codecov (npm package) before version 3.7.1 the upload method has a command injection vulnerability. Clients of the co

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codecov	Codecov	All	All	All	All
Application	Codecov	Codecov	All	All	All	All

References

Reference	Source
codecov NPM module allows remote attackers to execute arbitrary commands · CVE-2020-7597 · GitHub Advisory Database · GitHub	MISC
Switch from execSync to execFileSync (#180) · codecov/codecov-node@c0711c6 · GitHub	MISC
Switch from execSync to execFileSync by drazisil · Pull Request #180 · codecov/codecov-node · GitHub	MISC
Problem loading page	MISC
Command injection in upload method · Advisory · codecov/codecov-node · GitHub	CONFIRMED
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983189](#) Nodejs (npm) Security Update for codecov (GHSA-xp63-6vf5-xf3v)

© [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](#)