



CVE-2022-25923

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

Summary

CVE	CVE-2022-25923
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-06 05:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	Versions of the package exec-local-bin before 1.2.0 are vulnerable to Command Injection via the theProcess() functionality

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exec-local-bin Project	Exec-local-bin	All	All	All	All

References

Reference	Source	Link
fixes(CVE-2022-25923): resolves command injection security issue · saeedseyfi/exec-local-bin@d425866 · GitHub	MISC	github.com
Command Injection in exec-local-bin CVE-2022-25923 Snyk	MISC	security.snyk.com
github.com/saeedseyfi/exec-local-bin/blob/92db00bde9d6e2d83410849f898df1...	MISC	github.com
exec-local-bin/index.js at 92db00bde9d6e2d83410849f898df12f075b73b0 · saeedseyfi/exec-local-bin · GitHub	MITRE	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.

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