



CVE-2020-4045

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

Summary

CVE	CVE-2020-4045
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-11 22:15:00 UTC
Updated	2020-06-17 17:28:00 UTC
Description	SSB-DB version 20.0.0 has an information disclosure vulnerability. The get() method is supposed to only decrypt messages

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scuttlebutt	Ssb-db	20.0.0	All	All	All
Application	Scuttlebutt	Ssb-db	20.0.0	All	All	All

References

Reference	Source	Link	Tags
Merge pull request from GHSA-mpgr-2cx9-327h · ssbc/ssb-db@43334d0 · GitHub	MISC	github.com	Patch, Third Party Advisory
SSB-DB#get() is decrypting messages by default · Advisory · ssbc/ssb-db · GitHub	CONFIRM	github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983867](#) Nodejs (npm) Security Update for ssb-db (GHSA-mpgr-2cx9-327h)

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