



CVE-2023-46233

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

Summary

CVE	CVE-2023-46233
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 21:15:00 UTC
Updated	2023-11-06 19:49:00 UTC
Description	crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than orig

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crypto-js Project	Crypto-js	All	All	All	All

References

Reference

- Change default hash algorithm and iteration's for PBKDF2 to prevent w... · brix/crypto-js@421dd53 · GitHub
- crypto-js PBKDF2 1,000 times weaker than specified in 1993 and 1.3M times weaker than current standard · Advisory · brix/crypto-js · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 6000354 Debian Security Update for cryptojs (DLA 3669-1)
- 995721 NodeJs (Npm) Security Update for crypto-js (GHSA-xwcq-pm8m-c4vf)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)