CVE-2023-46234

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-46234
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-26 15:15:00 UTC
Updated	2023-11-07 19:57:00 UTC
Description	browserify-sign is a package to duplicate the functionality of node's crypto public key functions, much of this is based on Fe

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Browserify	Browserify-sign	All	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All

References

Reference	Source
Debian -- Security Information -- DSA-5539-1 node-browserify-sign	MISC
An upper bound check issue in `dsaVerify` leads to a signature forgery attack · Advisory · browserify/browserify-sign · GitHub	MISC
[Fix] properly check the upper bound for DSA signatures · browserify/browserify-sign@85994cd · GitHub	MISC
[SECURITY] [DLA 3635-1] node-browserify-sign security update	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

284943 Fedora Security Update for yarnpkg (FEDORA-2024-5ecc250449)

284965 Fedora Security Update for yarnpkg (FEDORA-2024-28fc0c2ef4)

6000260 Debian Security Update for node-browserify-sign (DLA 3635-1)

6000302 Debian Security Update for node-browserify-sign (DSA 5539-1)

995754 NodeJs (Npm) Security Update for browserify-sign (GHSA-x9w5-v3q2-3rhw)