CVE-2020-28498

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-28498
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-02 19:15:00 UTC
Updated	2021-02-08 17:35:00 UTC
Description	The package elliptic before 6.5.4 are vulnerable to Cryptographic Issues via the secp256k1 implementation in elliptic/ec/key

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elliptic Project	Elliptic	All	All	All	All
Application	Elliptic Project	Elliptic	All	All	All	All

References

Reference	Source	Link	Tags
ec: validate that a point before deriving keys · indutny/elliptic@441b742 · GitHub	CONFIRM	github.com	Patch, Third Party Advisory
blog/secp256k1_twist_attacks.md at master · christianlundkvist/blog · GitHub	MISC	github.com	Third Party Advisory
Cryptographic Issues in org.webjars.npm:elliptic | Snyk	CONFIRM	snyk.io	Patch, Third Party Advisory
Cryptographic Issues in elliptic | Snyk	MISC	snyk.io	Patch, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Kyle Den Hartog

Legacy QID Mappings

982924 Nodejs (npm) Security Update for elliptic (GHSA-r9p9-mrjm-926w)

© 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 registred 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