CVE-2020-13822

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13822
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 15:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading '\0' bytes, or i

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elliptic Project	Elliptic	6.5.2	All	All	All
Application	Elliptic Project	Elliptic	6.5.2	All	All	All

References

Reference	Sour
elliptic	MISC
Malleability-Attack: Why It Matters – Herman Schoenfeld – Medium	MISC
How Not to Use ECDSA – Learning Words	MISC
Lack of encoding checks allows a certain degree of signature malleability in ECDSA signatures · Issue #226 · indutny/elliptic · GitHub	MISC
Malleability-Attack: Why It Matters | by Herman Schoenfeld | Medium	
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

980730 Nodejs (npm) Security Update for elliptic (GHSA-vh7m-p724-62c2)