CVE-2020-14966

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-14966
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-22 12:15:00 UTC
Updated	2023-01-28 00:57:00 UTC
Description	An issue was discovered in the jsrsasign package through 8.0.18 for Node.js. It allows a malleability in ECDSA signatures b

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jsrsasign Project	Jsrsasign	All	All	All	All
Application	Netapp	Max Data	-	All	All	All

References

Reference	So
June 2020 Node.js Vulnerabilities in NetApp Products | NetApp Product Security	CC
Release RSA decryption and RSA signature validation maleability fix · kjur/jsrsasign · GitHub	MI
Lack of encoding checking in jsrsasign allows a certain degree of malleability in ECDSA signatures · Issue #437 · kjur/jsrsasign · GitHub	MI
Release RSAPSS verification maleability fix and others · kjur/jsrsasign · GitHub	MI
jsrsasign	MI
jsrsasign - cryptography library in JavaScript	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980503 Nodejs (npm) Security Update for jsrsasign (GHSA-p8c3-7rj8-q963)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**