CVE-2020-14967

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

Summary

CVE	CVE-2020-14967
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 before 8.0.18 for Node.js. Its RSA PKCS1 v1.5 decryption implementatio

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
June 2020 Node.js Vulnerabilities in NetApp Products | NetApp Product Security
Release RSA decryption and RSA signature validation maleability fix · kjur/jsrsasign · GitHub
The RSA PKCS1 v1.5 decryption implementation does not detect ciphertext modification (prepended 0's bytes to the ciphertext) · Issue #439 ·
Release RSAPSS verification maleability fix and others · kjur/jsrsasign · GitHub
jsrsasign
jsrsasign - cryptography library in JavaScript
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980500 Nodejs (npm) Security Update for jsrsasign (GHSA-xxxq-chmp-67g4)

Free CVE JSON API cve.report/api

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