



CVE-2020-14968

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-14968
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-22 12:15:00 UTC
Updated	2023-01-27 20:52:00 UTC
Description	An issue was discovered in the jsrsasign package before 8.0.17 for Node.js. Its RSASSA-PSS (RSA-PSS) implementation c

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](#)
- [Release RSAPSS verification maleability fix and others · kjur/jsrsasign · GitHub](#)
- [The RSA-PSS implementation does not detect signature modification \(prepending "0" bytes\) to the signature · Issue #438 · kjur/jsrsasign · GitH](#)
- [jsrsasign](#)
- [jsrsasign - cryptography library in JavaScript](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

980504 Nodejs (npm) Security Update for jsrsasign (GHSA-q3gh-5r98-j4h3)

© [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 registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)