



# CVE-2020-14966

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-14966
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-22 12:15:00 UTC
<b>Updated</b>	2023-01-28 00:57:00 UTC
<b>Description</b>	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	<a href="#">Jsrsasign Project</a>	<a href="#">Jsrsasign</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Max Data</a>	-	All	All	All

## References

Reference	Source
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

© [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](#)