



CVE-2022-25898

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

Summary

CVE	CVE-2022-25898
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-01 20:15:00 UTC
Updated	2022-07-13 19:01:00 UTC
Description	The package jsrsasign before 10.5.25 are vulnerable to Improper Verification of Cryptographic Signature when JWS or JWT

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

References

Reference	Source	Link
Improper Verification of Cryptographic Signature in org.webjars.npm:jsrsasign CVE-2022-25898 Snyk	CONFIRM	snyk.io
Improper Verification of Cryptographic Signature in org.webjars.bowergithub.kjur:jsrsasign CVE-2022-25898 Snyk	CONFIRM	snyk.io
Release CVE-2022-25898 Security fix in JWS and JWT validation · kjur/jsrsasign · GitHub	CONFIRM	github.co
Improper Verification of Cryptographic Signature in org.webjars.bower:jsrsasign CVE-2022-25898 Snyk	CONFIRM	snyk.io
CVE-2022-25898 Security fix in JWS and JWT validation · kjur/jsrsasign@4536a6e · GitHub	CONFIRM	github.co
Improper Verification of Cryptographic Signature in jsrsasign CVE-2022-25898 Snyk	CONFIRM	snyk.io
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

LEGACY: Adi Malyanker

LEGACY: Or David

There are currently no legacy QID mappings associated with this CVE.

© [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](#)