CVE-2026-4603

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

Summary

CVE	CVE-2026-4603
State	PUBLISHED
Assigner	snyk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 06:16:22 UTC
Updated	2026-04-29 01:00:01 UTC
Description	Versions of the package jsrsasign before 11.1.1 are vulnerable to Division by zero due to the RSASetPublic/KEYUTIL parsi

Risk And Classification

Primary CVSS: v4.0 2 LOW from report@snyk.io

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-369 | CWE-369 Division by zero

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	2	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	report@snyk.io	Secondary	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jsrsasign Project	Jsrsasign	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Jsrsasign	affected 11.1.1 semver	Not specified

References

Reference	Source	Link	Tags
security.snyk.io/vuln/SNYK-JS-JSRSASIGN-15371176	report@snyk.io	security.snyk.io	Third Party Advisory
github.com/kjur/jsrsasign/pull/649	report@snyk.io	github.com	Issue Tracking
github.com/kjur/jsrsasign/commit/dc41d49fac4297e7a737a3ef8ebd0aa9c49ef93f	report@snyk.io	github.com	Patch
gist.github.com/Kr0emer/5366b7364c4fbf7e754bc377f321e9f3	report@snyk.io	gist.github.com	Exploit, Mitigation, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Kr0emer (en)

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