Forge has signature forgery in RSA-PKCS due to ASN.1 extra field

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33894
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 21:17:25 UTC
Updated	2026-03-30 13:26:07 UTC
Description	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.4.0,

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

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

EPSS: 0.000290000 probability, percentile 0.081400000 (date 2026-04-01)

Problem Types: CWE-20 | CWE-347 | CWE-347 CWE-347: Improper Verification of Cryptographic Signature | CWE-20 CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Digitalbazaar	Forge	affected < 1.4.0	Not specified

References

Reference	Source	Link	Tags
github.com/digitalbazaar/forge/security/advisories/GHSA-ppp5-5v6c-4jwp	security-advisories@github.com	github.com	
www.rfc-editor.org/rfc/rfc8017.html	security-advisories@github.com	www.rfc-editor.org	
datatracker.ietf.org/doc/html/rfc2313	security-advisories@github.com	datatracker.ietf.org	
mailarchive.ietf.org/arch/msg/openpgp/5rnE9ZRN1AokBVj3VqblGIP63QE	security-advisories@github.com	mailarchive.ietf.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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