



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

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

## Summary

<b>CVE</b>	CVE-2026-33894
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 21:17:25 UTC
<b>Updated</b>	2026-03-30 13:26:07 UTC
<b>Description</b>	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

Integrity

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	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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.

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)