



CVE-2026-21713

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-21713
State	PUBLISHED
Assigner	hackerone
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 20:16:19 UTC
Updated	2026-05-10 14:16:47 UTC
Description	A flaw in Node.js HMAC verification uses a non-constant-time comparison when validating user-provided signatures, potent

Risk And Classification

Primary CVSS: v3.0 5.9 MEDIUM from support@hackerone.com

CVSS: 3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.000120000 probability, percentile 0.017070000 (date 2026-05-12)

Problem Types: CWE-208 | CWE-208 CWE-208 Observable Timing Discrepancy

Version	Source	Type	Score	Severity	Vector
3.0	support@hackerone.com	Secondary	5.9	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.0	CNA	DECLARED	5.9	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

None

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nodejs	Node	affected 20.20.1 20.20.1 semver	Not specified
CNA	Nodejs	Node	affected 22.22.1 22.22.1 semver	Not specified
CNA	Nodejs	Node	affected 24.14.0 24.14.0 semver	Not specified
CNA	Nodejs	Node	affected 25.8.1 25.8.1 semver	Not specified
CNA	Nodejs	Node	affected 4.0 4.* semver	Not specified
CNA	Nodejs	Node	affected 5.0 5.* semver	Not specified
CNA	Nodejs	Node	affected 6.0 6.* semver	Not specified
CNA	Nodejs	Node	affected 7.0 7.* semver	Not specified
CNA	Nodejs	Node	affected 8.0 8.* semver	Not specified
CNA	Nodejs	Node	affected 9.0 9.* semver	Not specified
CNA	Nodejs	Node	affected 10.0 10.* semver	Not specified
CNA	Nodejs	Node	affected 11.0 11.* semver	Not specified
CNA	Nodejs	Node	affected 12.0 12.* semver	Not specified
CNA	Nodejs	Node	affected 13.0 13.* semver	Not specified
CNA	Nodejs	Node	affected 14.0 14.* semver	Not specified
CNA	Nodejs	Node	affected 15.0 15.* semver	Not specified
CNA	Nodejs	Node	affected 16.0 16.* semver	Not specified
CNA	Nodejs	Node	affected 17.0 17.* semver	Not specified
CNA	Nodejs	Node	affected 18.0 18.* semver	Not specified
CNA	Nodejs	Node	affected 19.0 19.* semver	Not specified

References

Reference	Source	Link	Tags
nodejs.org/en/blog/vulnerability/march-2026-security-releases	support@hackerone.com	nodejs.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

This is a placeholder for a comment that has 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)