



Improper Verification of Cryptographic Signature in Elastic Package Registry Leading to Package Integrity Bypass

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

Summary

CVE	CVE-2026-33467
State	PUBLISHED
Assigner	elastic
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 22:16:48 UTC
Updated	2026-05-05 17:55:21 UTC
Description	Improper Verification of Cryptographic Signature (CWE-347) in Elastic Package Registry could allow an attacker positioned

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from security@elastic.co

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

EPSS: 0.000160000 probability, percentile 0.036600000 (date 2026-05-05)

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

Version	Source	Type	Score	Severity	Vector
3.1	security@elastic.co	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elastic	Elastic Package Registry	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Elastic	Elastic Package Registry	affected 0.1.0 1.37.0 semver	Not specified

References

Reference	Source	Link	Tags
discuss.elastic.co/t/elastic-package-registry-1-38-0-security-update-esa-2026-27...	security@elastic.co	discuss.elastic.co	Vendor Adviso
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report