Rust-rpm-sequoia: rust-rpm-sequoia: denial of service via crafted rpm file during signature verification

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-2625
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 19:17:22 UTC
Updated	2026-04-03 19:17:22 UTC
Description	A flaw was found in rust-rpm-sequoia. An attacker can exploit this vulnerability by providing a specially crafted Red Hat Pac

Risk And Classification

Primary CVSS: v3.1 4 MEDIUM from secalert@redhat.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat Hardened Images 1	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2026-2625	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
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: Red Hat would like to thank Yashashree Gund for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-02-17T13:07:17.107Z	Reported to Red Hat.
CNA	2026-02-17T12:34:00.000Z	Made public.

Workarounds

CNA: Avoid processing untrusted or attacker-controlled RPM files with rpm -Kv or rpm --checksig. Use isolated environments or additional validation layers when handling untrusted RPM artifacts.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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