



Bug 2440357 (CVE-2026-2625) - CVE-2026-2625 rust-rpm-sequoia: rust-rpm-sequoia: Denial of Service via crafted RPM file during signature verification

Keywords:

Reported: 2026-02-17 13:12 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-17 13:29 UTC ([History](#))

Alias: CVE-2026-2625

CC List: 0 users

Product: Security Response

Component: vulnerability

Fixed In Version:

Clone Of:

Version: unspecified

Environment:

Hardware: All

Last Closed:

Embargoed:

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-17 13:12:49 UTC

[Description](#)

A crafted RPM file can trigger a Rust panic in the OpenPGP signature parsing code (`librpm_sequoia`) during RPM signature verification. The panic crosses the Rust/C FFI boundary and causes an unconditional abort of the `rpm` process, resulting in a denial of service. The issue is reachable via standard RPM CLI operations such as `rpm -Kv` and `rpm --checksig` without installing the package.

An attacker only needs to supply a specially crafted RPM file to a victim system where the RPM file is processed for signature verification (e.g., `rpm -Kv`, `rpm --checksig`, CI pipelines, or automated package validation workflows). No privileges, user interaction, or package installation are

required.

Note

You need to [log in](#) before you can comment on or make changes to this bug.

