



# Libssh: libssh: denial of service via improper configuration file handling

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-0965   |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | redhat  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-03-26 21:17:00 UTC   |
| <b>Updated</b>         | 2026-04-02 17:33:46 UTC   |
| <b>Description</b>     | A flaw was found in libssh where it can attempt to open arbitrary files during configuration parsing. A local attacker can exploit this to cause a denial of service. |

## Risk And Classification

**Primary CVSS:** v3.0 3.3 LOW from secalert@redhat.com

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

**EPSS:** 0.000160000 probability, percentile 0.034920000 (date 2026-04-02)

**Problem Types:** CWE-73 | CWE-73 External Control of File Name or Path

| Version | Source              | Type      | Score | Severity | Vector                                       |
|---------|---------------------|-----------|-------|----------|--|
| 3.0     | secalert@redhat.com | Secondary | 3.3   | LOW      | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L |
| 3.0     | CNA                 | CVSS      | 3.3   | LOW      | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L |

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

#### NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product          | Version | Update | Edition | Language |
|------------------|--------|------------------|---------|--------|---------|----------|
| Application      | Libssh | Libssh           | All     | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 10.0    | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 9.0     | All    | All     | All      |

#### 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 6             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 7             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 8             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 9             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat OpenShift Container Platform 4 | Not specified | Not specified |

#### References

| Reference   | Source              | Link  | Tags                 |
|---|---------------------|---|----------------------|
| <a href="https://access.redhat.com/security/cve/CVE-2026-0965">access.redhat.com/security/cve/CVE-2026-0965</a> | secalert@redhat.com | <a href="https://access.redhat.com">access.redhat.com</a>     | Third Party Advisory |
| <a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>                         | secalert@redhat.com | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a> | Third Party Advisory |
| CVE Program record  | CVE.ORG             | <a href="https://www.cve.org">www.cve.org</a>                 | canonical            |
| NVD vulnerability detail  | NVD                 | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               | canonical, analysis  |

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Red Hat would like to thank Jakub Jelen (libssh) and Kang Yang for reporting this issue.  
(en)

#### Additional Advisory Data

| Source | Time                     | Event                |
|--------|--------------------------|----------------------|
| CNA    | 2026-02-04T23:40:45.160Z | Reported to Red Hat. |
| CNA    | 2026-02-10T18:47:22.524Z | Made public.         |

## Workarounds

**CNA:** Ensure the client and server are using only regular files as configuration.

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](#)