Libssh: libssh: denial of service via inefficient regular expression processing

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-0967
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 21:17:00 UTC
Updated	2026-04-02 17:28:27 UTC
Description	A flaw was found in libssh. A remote attacker, by controlling client configuration files or known_hosts files, could craft specif

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000680000 probability, percentile 0.209940000 (date 2026-04-02)

Problem Types: CWE-1333 | CWE-1333 Inefficient Regular Expression Complexity

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.0	secalert@redhat.com	Secondary	2.2	LOW	CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:L
3.0	CNA	CVSS	2.2	LOW	CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:L/AC:H/PR:L/UI:R/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
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Third Party Advisory
www.libssh.org/2026/02/10/libssh-0-12-0-and-0-11-4-security-releases	secalert@redhat.com	www.libssh.org	Release Notes
access.redhat.com/security/cve/CVE-2026-0967	secalert@redhat.com	access.redhat.com	Third Party Advisory
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 Jakub Jelen (libssh) and Kang Yang for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-02-04T23:43:23.869Z	Reported to Red Hat.
CNA	2026-02-10T18:47:09.215Z	Made public.

Workarounds

CNA: Avoid using complex patterns in configuration files and known_hosts.

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