Libssh: improper sanitation of paths received from scp servers

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-0964
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 21:17:00 UTC
Updated	2026-03-30 13:26:50 UTC
Description	A malicious SCP server can send unexpected paths that could make the client application override local files outside of wor

Risk And Classification

Primary CVSS: v3.0 5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000340000 probability, percentile 0.099230000 (date 2026-04-01)

Problem Types: CWE-22 | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.0	secalert@redhat.com	Secondary	5	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L
3.0	CNA	CVSS	5	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/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 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	
www.libssh.org/2026/02/10/libssh-0-12-0-and-0-11-4-security-releases	secalert@redhat.com	www.libssh.org	
access.redhat.com/security/cve/CVE-2026-0964	secalert@redhat.com	access.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 CTyun (Red-Shield Security Lab) and Jakub Jelen (libssh) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-02-04T23:37:53.443Z	Reported to Red Hat.
CNA	2026-02-10T18:44:42.346Z	Made public.

Workarounds

CNA: Do not use SCP! SCP is deprecated for several years and will be removed in future releases! If you have to, the application MUST validate the path returned from `ssh_scp_request_get_filename()` is the path the application requested. The libssh does not

do any writing in this case.

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 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