



Libssh: buffer underflow in ssh_get_hexa() on invalid input

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

Summary

CVE	CVE-2026-0966
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 The API function `ssh_get_hexa()` is vulnerable, when 0-length input is provided to this function. This function is used inter

Risk And Classification

Primary CVSS: v3.0 6.5 MEDIUM from secalert@redhat.com

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

EPSS: 0.001030000 probability, percentile 0.283380000 (date 2026-04-02)

Problem Types: CWE-124 | CWE-124 Buffer Underwrite ('Buffer Underflow')

Version	Source	Type	Score	Severity	Vector
3.0	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.0	CNA	CVSS	6.5	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/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
access.redhat.com/security/cve/CVE-2026-0966	secalert@redhat.com	access.redhat.com	
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	
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), Jun Xu, Kang Yang, and Yunhang Zhang for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-01-26T23:14:46.617Z	Reported to Red Hat.
CNA	2026-02-10T18:47:15.531Z	Made public.

Workarounds

CNA: To mitigate this issue, consider disabling GSSAPI authentication if it is not required, or reduce the `LogLevel` in the `sshd_config` file to a value lower than `SSH_LOG_PACKET` (e.g., `INFO`). To disable GSSAPI authentication, add or modify the following line in `/etc/ssh/sshd_config`: `GSSAPIAuthentication no` To reduce logging verbosity, add or

modify the following line in `/etc/ssh/sshd_config`: `LogLevel INFO` After making changes to `sshd_config`, the `sshd` service must be restarted for the changes to take effect. This may temporarily interrupt active SSH sessions.

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](#)