CVE-2026-0966

VEX

Public on February 10, 2026

Last modified: April 30, 2026 at 4:36:49 PM UTC

MODERATE

Moderate severity

What does this mean?

6.5

CVSS v3 Score Breakdown

Jump to section

Description | Mitigation | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | Acknowledgements | FAQ

Description

The API function `ssh_get_hexa()` is vulnerable, when 0-lenght input is provided to this function. This function is used internally in `ssh_get_fingerprint_hash()` and `ssh_print_hexa()` (deprecated), which is vulnerable to the same input (length is provided by the calling application).

The function is also used internally in the gssapi code for logging the OIDs received by the server during GSSAPI authentication. This could be triggered remotely, when the server allows GSSAPI authentication and logging verbosity is set at least to

SSH_LOG_PACKET (3). This could cause self-DoS of the per-connection daemon process.

Mitigation

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.

Additional information

- Bugzilla 2433121: libssh: Buffer underflow in ssh_get_hexa() on invalid input
- CWE-124: Buffer Underwrite ('Buffer Underflow')

External references

- https://www.cve.org/CVERecord?id=CVE-2026-0966
- https://nvd.nist.gov/vuln/detail/CVE-2026-0966
- https://www.libssh.org/2026/02/10/libssh-0-12-0-and-0-11-4-security-releases/

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State | Errata | Clear all

Products / Services	Red Hat Hardened Images
Components	libssh-main
State	Fixed
Justification	None
Errata	RHSA-2026:7067
Release Date	April 8, 2026

Products / Services	Red Hat Enterprise Linux 10
Components	libssh
State	Affected
Justification	None
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 6
Components	libssh2
State	Not affected
Justification	Vulnerable Code not Present
Errata	

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	6.5	8.2	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	Low	Low	N/A
Privileges Required	None	None	N/A
User Interaction	None	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	None	None	N/A
Integrity Impact	Low	Low	N/A

	Red Hat	NVD	CVE List
Availability Impact	Low	High	N/A

CVSS v3 Vector

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

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

Acknowledgements

Red Hat would like to thank Jakub Jelen (libssh), Jun Xu, Kang Yang, and Yunhang Zhang for reporting this issue.

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors?

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?

What can I do if my product is listed as "Will not fix"?

What can I do if my product is listed as "Fix deferred"?

What is a mitigation?

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: April 30, 2026 at 4:36:49 PM UTC