Cookie Preferences and Opt-Out Rights
Your Choices About Cookies on this Site

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or “targeted advertising” under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser’s global privacy settings,

CVE

VEX

Public or

Last mo

Descrip

s FAQ

Descr

The AP

to this

functio

ssh_pr

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 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	
Release Date	

Products / Services	Red Hat Enterprise Linux 7
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).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

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

	Red Hat	NVD	CVE List
Availability Impact	Low	N/A	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

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: March 26, 2026 at 9:08:52 PM UTC