



# CVE-2023-6918

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

## Summary

<b>CVE</b>	CVE-2023-6918
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-12-19 00:15:00 UTC
<b>Updated</b>	2024-01-04 20:21:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-252

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	All	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	-	All	All	All
Application	<a href="#">Libssh2</a>	<a href="#">Libssh2</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All

## References

Reference	Source	Link	Tags
<a href="http://www.libssh.org/security/advisories/CVE-2023-6918.txt">www.libssh.org/security/advisories/CVE-2023-6918.txt</a>		<a href="http://www.libssh.org">www.libssh.org</a>	Vendor Advis
<a href="https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message...">lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...</a>		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Mailing List, V
<a href="#">RHBZ#2254997</a>		<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Trackin
<a href="https://access.redhat.com/security/cve/CVE-2023-6918">access.redhat.com/security/cve/CVE-2023-6918</a>		<a href="https://access.redhat.com">access.redhat.com</a>	Mailing List, V
<a href="http://www.libssh.org/2023/12/18/libssh-0-10-6-and-libssh-0-9-8-security-releases">www.libssh.org/2023/12/18/libssh-0-10-6-and-libssh-0-9-8-security-releases</a>		<a href="http://www.libssh.org">www.libssh.org</a>	Release Note
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, an

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

200060	Ubuntu Security Notification for libssh Vulnerabilities (USN-6592-1)
200095	Ubuntu Security Notification for libssh Vulnerabilities (USN-6592-2)
285088	Fedora Security Update for libssh (FEDORA-2023-0733306be9)
506112	Alpine Linux Security Update for libssh
6000408	Debian Security Update for libssh (DSA 5591-1)
673335	EulerOS Security Update for libssh (EulerOS-SA-2024-1316)
673381	EulerOS Security Update for libssh (EulerOS-SA-2024-1338)
673472	EulerOS Security Update for libssh (EulerOS-SA-2024-1197)
673750	EulerOS Security Update for libssh (EulerOS-SA-2024-1216)
673785	EulerOS Security Update for libssh (EulerOS-SA-2024-1177)
674082	EulerOS Security Update for libssh (EulerOS-SA-2024-1238)
755620	SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0140-1)
755778	SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0525-1)
755806	SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
907721	Common Base Linux Mariner (CBL-Mariner) Security Update for libssh (32199-1)

© [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](#)