



# CVE-2021-3634

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

## Summary

<b>CVE</b>	CVE-2021-3634
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-31 17:15:00 UTC
<b>Updated</b>	2023-12-22 10:15:00 UTC
<b>Description</b>	A flaw has been found in libssh in versions prior to 0.9.6. The SSH protocol keeps track of two shared secrets during the life

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql Workbench</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All

## References

Reference	Source	Link
CVE-2021-3634 libssh Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
[SECURITY] Fedora 35 Update: libssh-0.9.6-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-4965-1 libssh	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
[SECURITY] Fedora 35 Update: libssh-0.9.6-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>

1978810 – (CVE-2021-3634) CVE-2021-3634 libssh: possible heap-based buffer overflow when rekeying	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
[SECURITY] Fedora 34 Update: libssh-0.9.6-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Oracle Critical Patch Update Advisory - January 2022	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
[SECURITY] Fedora 33 Update: libssh-0.9.6-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: libssh-0.9.6-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
libssh: Multiple Vulnerabilities (GLSA 202312-05) — Gentoo security		<a href="https://security.gentoo.org">security.gentoo.org</a>
[SECURITY] Fedora 34 Update: libssh-0.9.6-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159812</a> Oracle Enterprise Linux Security Update for libssh (ELSA-2022-2031)
<a href="#">178780</a> Debian Security Update for libssh (DSA 4965-1)
<a href="#">183967</a> Debian Security Update for libssh (CVE-2021-3634)
<a href="#">198472</a> Ubuntu Security Notification for libssh Vulnerability (USN-5053-1)
<a href="#">240324</a> Red Hat Update for libssh security (RHSA-2022:2031)
<a href="#">281933</a> Fedora Security Update for libssh (FEDORA-2021-288925ac19)
<a href="#">281965</a> Fedora Security Update for libssh (FEDORA-2021-f2a020a065)
<a href="#">501876</a> Alpine Linux Security Update for libssh
<a href="#">670827</a> EulerOS Security Update for libssh (EulerOS-SA-2021-2716)
<a href="#">670945</a> EulerOS Security Update for libssh (EulerOS-SA-2021-2691)
<a href="#">690031</a> Free Berkeley Software Distribution (FreeBSD) Security Update for libssh (57b1ee25-1a7c-11ec-9376-0800272221cc)
<a href="#">710806</a> Gentoo Linux libssh Multiple Vulnerabilities (GLSA 202312-05)
<a href="#">755806</a> SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
<a href="#">901107</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libssh (7274)
<a href="#">940503</a> AlmaLinux Security Update for libssh (ALSA-2022:2031)
<a href="#">960135</a> Rocky Linux Security Update for libssh (RLSA-2022:2031)

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](#)**