



# CVE-2019-14889

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

## Summary

<b>CVE</b>	CVE-2019-14889
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-10 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:05:00 UTC
<b>Description</b>	A flaw was found with the libssh API function ssh_scp_new() in versions before 0.9.3 and before 0.8.8. When the libssh SC

## Risk And Classification

**Problem Types: CWE-78**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
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	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql Workbench</a>	All	All	All	All

## References

Reference	Source
[SECURITY] Fedora 31 Update: libssh-0.9.3-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
libssh: Arbitrary command execution (GLSA 202003-27) — Gentoo security	GENTOO
<a href="http://www.libssh.org/security/advisories/CVE-2019-14889.txt">www.libssh.org/security/advisories/CVE-2019-14889.txt</a>	CONFIRM
[SECURITY] [DLA 3437-1] libssh security update	MLIST
USN-4219-1: libssh vulnerability   Ubuntu security notices	UBUNTU
[SECURITY] Fedora 31 Update: libssh-0.9.3-1.fc31 - package-announce - Fedora Mailing-Lists	
[SECURITY] [DLA 2038-1] libssh security update	MLIST
1772523 – (CVE-2019-14889) CVE-2019-14889 libssh: unsanitized location in scp could lead to unwanted command execution	CONFIRM
[SECURITY] Fedora 30 Update: libssh-0.9.3-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
[security-announce] openSUSE-SU-2019:2689-1: important: Security update	SUSE
[SECURITY] Fedora 30 Update: libssh-0.9.3-1.fc30 - package-announce - Fedora Mailing-Lists	
Oracle Critical Patch Update Advisory - April 2020	N/A
[security-announce] openSUSE-SU-2020:0102-1: important: Security update	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">181812</a> Debian Security Update for libssh (DLA 3437-1)
<a href="#">377559</a> Alibaba Cloud Linux Security Update for libssh (ALINUX3-SA-2022:0067)
<a href="#">501062</a> Alpine Linux Security Update for libssh
<a href="#">755806</a> SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
<a href="#">770068</a> Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)
<a href="#">940406</a> AlmaLinux Security Update for libssh (ALSA-2020:4545)
<a href="#">960879</a> Rocky Linux Security Update for libssh (RLSA-2020:4545)

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](#)**