



# CVE-2019-3862

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

## Summary

<b>CVE</b>	CVE-2019-3862
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-21 16:01:00 UTC
<b>Updated</b>	2023-11-07 03:10:00 UTC
<b>Description</b>	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets w

## Risk And Classification

**Problem Types:** CWE-125

## 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>	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>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Application	<a href="#">Libssh2</a>	<a href="#">Libssh2</a>	All	All	All	All
Application	<a href="#">Libssh2</a>	<a href="#">Libssh2</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All

## References

Reference
<a href="#">Red Hat Customer Portal</a>
<a href="#">[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists</a>
<a href="#">Broadcom Inc.   Connecting Everything</a>
<a href="#">Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update</a>

oss-security - [SECURITY ADVISORIES] libssh2
March 2019 Libssh2 Vulnerabilities in NetApp Products   NetApp Product Security
Debian -- Security Information -- DSA-4431-1 libssh2
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 29 Update: libssh2-1.8.1-1.fc29 - package-announce - Fedora Mailing-Lists
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f
1687312 – (CVE-2019-3862) CVE-2019-3862 libssh2: Out-of-bounds memory comparison with specially crafted message channel request
Slackware Security Advisory - libssh2 Updates ≈ Packet Storm
[SECURITY] [DLA 1730-1] libssh2 security update
libssh2 Multiple Security Vulnerabilities
libssh2 Security Advisory: CVE-2019-3862
[SECURITY] Fedora 29 Update: libssh2-1.8.1-1.fc29 - package-announce - Fedora Mailing-Lists
Oracle Critical Patch Update - October 2019
Oracle Critical Patch Update Advisory - January 2020
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f
Bugtraq: [slackware-security] libssh2 (SSA:2019-077-01)
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [377515](#) Alibaba Cloud Linux Security Update for libssh2 (ALINUX2-SA-2019:0048)
- [500318](#) Alpine Linux Security Update for libssh2
- [504085](#) Alpine Linux Security Update for libssh2
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- [750528](#) OpenSUSE Security Update for libssh2\_org (openSUSE-SU-2020:2129-1)
- [750530](#) OpenSUSE Security Update for libssh2\_org (openSUSE-SU-2020:2126-1)

© 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](#).

