



CVE-2019-3861

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-3861
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-25 19:29:00 UTC
Updated	2023-11-07 03:10:00 UTC
Description	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length were processed.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libssh2	Libssh2	All	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update	BUGTRAQ	seclists.org
1687311 – (CVE-2019-3861) CVE-2019-3861 libssh2: Out-of-bounds reads with specially crafted SSH packets	CONFIRM	bugzilla.redhat.com
March 2019 Libssh2 Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Debian -- Security Information -- DSA-4431-1 libssh2	DEBIAN	www.debian.org

[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproj
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f	SUSE	lists.opensuse
libssh2 Security Advisory: CVE-2019-3861	MISC	www.libssh2.o
[SECURITY] [DLA 1730-1] libssh2 security update	MLIST	lists.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.
Oracle Critical Patch Update - October 2019	MISC	www.oracle.co
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f	SUSE	lists.opensuse
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [377521](#) Alibaba Cloud Linux Security Update for libssh2 (ALINUX2-SA-2019:0100)
- [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](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report