



CVE-2019-3858

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

Summary

CVE	CVE-2019-3858
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 21:29:00 UTC
Updated	2023-11-07 03:10:00 UTC
Description	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from th

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
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Application	Libssh2	Libssh2	All	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
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists
Broadcom Inc. Connecting Everything

Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update
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
libssh2 Security Advisory: CVE-2019-3858
1687306 – (CVE-2019-3858) CVE-2019-3858 libssh2: Zero-byte allocation with a specially crafted SFTP packed leading to an out-of-bounds r
[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
Slackware Security Advisory - libssh2 Updates ≈ Packet Storm
[SECURITY] [DLA 1730-1] libssh2 security update
libssh2 Multiple Security Vulnerabilities
[SECURITY] Fedora 29 Update: libssh2-1.8.1-1.fc29 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal
Oracle Critical Patch Update - October 2019
[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

- [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, 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](#)