CVE-2019-3860

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-3860
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 SFTP packets with empty payloads are parse

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.fedorapr
Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update	BUGTRAQ	seclists.org
[security-announce] openSUSE-SU-2019:1640-1: moderate: Security update f	SUSE	lists.opensus
March 2019 Libssh2 Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netap
Debian -- Security Information -- DSA-4431-1 libssh2	DEBIAN	www.debian.(

[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedorapr
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f	SUSE	lists.opensus
libssh2 Security Advisory: CVE-2019-3860	MISC	www.libssh2.
1687310 – (CVE-2019-3860) CVE-2019-3860 libssh2: Out-of-bounds reads with specially crafted SFTP packets	CONFIRM	bugzilla.redha
[SECURITY] [DLA 1730-1] libssh2 security update	MLIST	lists.debian.o
Oracle Critical Patch Update - October 2019	MISC	www.oracle.c
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f	SUSE	lists.opensus
[SECURITY] [DLA 1730-4] libssh2 regression update	MLIST	lists.debian.o
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

- 355094 Amazon Linux Security Advisory for libssh2 : ALAS2-2023-2046
- 355347 Amazon Linux Security Advisory for libssh2 : ALAS-2023-1756
- 355524 Amazon Linux Security Advisory for libssh2 : AL2012-2023-423
- 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)