CVE-2019-3857

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-3857
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 integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_

Risk And Classification

Problem Types: CWE-787 | CWE-190

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	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	28	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
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All

Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	S
Red Hat Customer Portal	R
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	
Red Hat Customer Portal	R
Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update	B
Red Hat Customer Portal	R
1687305 – (CVE-2019-3857) CVE-2019-3857 libssh2: Integer overflow in SSH packet processing channel resulting in out of bounds write	C
March 2019 Libssh2 Vulnerabilities in NetApp Products | NetApp Product Security	C
Debian -- Security Information -- DSA-4431-1 libssh2	D
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	F
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f	S
Red Hat Customer Portal	R
[SECURITY] [DLA 1730-1] libssh2 security update	M
libssh2 Security Advisory: CVE-2019-3857	M
Red Hat Customer Portal	R
Oracle Critical Patch Update - October 2019	M
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f	S
Red Hat Customer Portal	R
CVE Program record	C

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 377077 Alibaba Cloud Linux Security Update for libssh2 (ALINUX2-SA-2019:0018)
- 378237 Virtuozzo Linux Security Update for libssh2-docs (VZLSA-2019:1652)
- 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)