CVE-2020-1730

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1730
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-13 19:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A flaw was found in libssh versions before 0.8.9 and before 0.9.4 in the way it handled AES-CTR (or DES ciphers if enablec

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Libssh	Libssh	All	All	All	All
Application	Libssh	Libssh	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Oracle	Mysql Workbench	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 31 Update: libssh-0.9.4-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedorapr
[SECURITY] Fedora 31 Update: libssh-0.9.4-2.fc31 - package-announce - Fedora Mailing-Lists		lists.fedorapr
CVE-2020-1730 Libssh Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.neta

Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.c
www.libssh.org/security/advisories/CVE-2020-1730.txt	MISC	www.libssh.c
1801998 – (CVE-2020-1730) CVE-2020-1730 libssh: denial of service when handling AES-CTR (or DES) ciphers	CONFIRM	bugzilla.redh
[SECURITY] Fedora 32 Update: libssh-0.9.4-2.fc32 - package-announce - Fedora Mailing-Lists		lists.fedorapr
USN-4327-1: libssh vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.c
[SECURITY] Fedora 32 Update: libssh-0.9.4-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedorapr
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

- 377559 Alibaba Cloud Linux Security Update for libssh (ALINUX3-SA-2022:0067)
- 501063 Alpine Linux Security Update for libssh
- 755806 SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
- 770068 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)
- 940406 AlmaLinux Security Update for libssh (ALSA-2020:4545)
- 960879 Rocky Linux Security Update for libssh (RLSA-2020:4545)