CVE-2021-3634

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3634
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-31 17:15:00 UTC
Updated	2023-12-22 10:15:00 UTC
Description	A flaw has been found in libssh in versions prior to 0.9.6. The SSH protocol keeps track of two shared secrets during the life

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	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
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Source	Link
CVE-2021-3634 libssh Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 35 Update: libssh-0.9.6-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Debian -- Security Information -- DSA-4965-1 libssh	DEBIAN	www.debian.org
[SECURITY] Fedora 35 Update: libssh-0.9.6-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org

1978810 – (CVE-2021-3634) CVE-2021-3634 libssh: possible heap-based buffer overflow when rekeying	MISC	bugzilla.redhat.com
[SECURITY] Fedora 34 Update: libssh-0.9.6-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com
[SECURITY] Fedora 33 Update: libssh-0.9.6-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 33 Update: libssh-0.9.6-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
libssh: Multiple Vulnerabilities (GLSA 202312-05) — Gentoo security		security.gentoo.org
[SECURITY] Fedora 34 Update: libssh-0.9.6-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
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

- 159812 Oracle Enterprise Linux Security Update for libssh (ELSA-2022-2031)
- 178780 Debian Security Update for libssh (DSA 4965-1)
- 183967 Debian Security Update for libssh (CVE-2021-3634)
- 198472 Ubuntu Security Notification for libssh Vulnerability (USN-5053-1)
- 240324 Red Hat Update for libssh security (RHSA-2022:2031)
- 281933 Fedora Security Update for libssh (FEDORA-2021-288925ac19)
- 281965 Fedora Security Update for libssh (FEDORA-2021-f2a020a065)
- 501876 Alpine Linux Security Update for libssh
- 670827 EulerOS Security Update for libssh (EulerOS-SA-2021-2716)
- 670945 EulerOS Security Update for libssh (EulerOS-SA-2021-2691)
- 690031 Free Berkeley Software Distribution (FreeBSD) Security Update for libssh (57b1ee25-1a7c-11ec-9376-0800272221cc)
- 710806 Gentoo Linux libssh Multiple Vulnerabilities (GLSA 202312-05)
- 755806 SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
- 901107 Common Base Linux Mariner (CBL-Mariner) Security Update for libssh (7274)
- 940503 AlmaLinux Security Update for libssh (ALSA-2022:2031)
- 960135 Rocky Linux Security Update for libssh (RLSA-2022:2031)

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