



CVE-2020-16135

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

Summary

CVE	CVE-2020-16135
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-29 21:15:00 UTC
Updated	2023-11-07 03:18:00 UTC
Description	libssh 0.9.4 has a NULL pointer dereference in tftpsrv.c if ssh_buffer_new returns NULL.

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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Libssh	Libssh	0.9.4	All	All	All
Application	Libssh	Libssh	0.9.4	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.15.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 32 Update: libssh-0.9.5-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 2303-1] libssh security update	MLIST	lists.debian.org	Third Party
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
⚓ T232 [sftpsrv] NULL pointer deref	MISC	bugs.libssh.org	Issue Tracker
libssh: Denial of Service (GL SA 202011 05) - Gentoo security	GENTOO	security.gentoo.org	

libssh: Denial of Service (CVE-2021-1103) — Gentoo Security	GENTOO	security.gentoo.org	
USN-4447-1: libssh vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[SECURITY] Fedora 33 Update: libssh-0.9.5-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
rLIBSSHe631ebb3e224	MISC	bugs.libssh.org	Exploit
Add missing return checks (!120) · Merge Requests · libssh project / libssh-mirror · GitLab	MISC	gitlab.com	Third F
[SECURITY] Fedora 32 Update: libssh-0.9.5-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: libssh-0.9.5-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159504](#) Oracle Enterprise Linux Security Update for libssh (ELSA-2021-4387)
- [239795](#) Red Hat Update for libssh (RHSA-2021:4387)
- [501064](#) Alpine Linux Security Update for libssh
- [501611](#) Alpine Linux Security Update for libssh
- [755806](#) SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
- [940260](#) AlmaLinux Security Update for libssh (ALSA-2021:4387)
- [960764](#) Rocky Linux Security Update for libssh (RLSA-2021:4387)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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