



CVE-2018-18585

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

Summary

CVE	CVE-2018-18585
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-23 02:29:00 UTC
Updated	2022-10-25 16:47:00 UTC
Description	chmd_read_headers in mspack/chmd.c in libmspack before 0.8alpha accepts a filename that has '\0' as its first or second c

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
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	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
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	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Kyzer	Libmspack	0.3	alpha	All	All
Application	Kyzer	Libmspack	0.4	alpha	All	All
Application	Kyzer	Libmspack	0.5	alpha	All	All
Application	Kyzer	Libmspack	0.6	alpha	All	All
Application	Kyzer	Libmspack	0.7	alpha	All	All

Application	Kyzer	Libmspack	0.3	alpha	All	All
Application	Kyzer	Libmspack	0.4	alpha	All	All
Application	Kyzer	Libmspack	0.5	alpha	All	All
Application	Kyzer	Libmspack	0.6	alpha	All	All
Application	Kyzer	Libmspack	0.7	alpha	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	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 Workstation	7.0	All	All	All
Application	Starwindsoftware	Starwind Virtual San	-	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	12	ga	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	12	ga	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All

References

Reference

[CVE-2018-18585 | SUSE](#)

[USN-3814-2: ClamAV vulnerabilities | Ubuntu security notices](#)

[#911637 - libmspack: CVE-2018-18585: Avoid returning CHM file entries that are "blank" because they have embedded null bytes - Debian Bu](#)

[Red Hat Customer Portal](#)

[oss-security - Buffer overflow in cabextract/libmspack \(Fwd: New cabextract 1.8 and libmspack 0.8 release\)](#)

[USN-3814-1: libmspack vulnerabilities | Ubuntu security notices](#)

[\[SECURITY\] \[DLA 1555-1\] libmspack security update](#)

[USN-3814-3: ClamAV vulnerabilities | Ubuntu security notices](#)

[cabextract, libmspack: Multiple vulnerabilities \(GLSA 201903-20\) — Gentoo security](#)

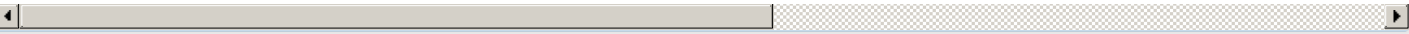
[Avoid returning CHM file entries that are "blank" because they have e... · kyz/libmspack@8759da8 · GitHub](#)

[libmspack chmd_read_headers Function Denial of Service Vulnerability](#)

[CVE-2018-18585 libmspack vulnerability in StarWind VSAN for vSphere \(VSA\)](#)

[CVE-2018-18585 - Red Hat Customer Portal](#)

[CVE-2018-18585](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377542](#) Alibaba Cloud Linux Security Update for libmspack (ALINUX2-SA-2019:0071)

[501044](#) Alpine Linux Security Update for libmspack

[710187](#) Gentoo Linux cabextract, libmspack Multiple vulnerabilities (GLSA 201903-20)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)