



# CVE-2018-14679

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-14679
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-28 23:29:00 UTC
<b>Updated</b>	2021-04-26 11:45:00 UTC
<b>Description</b>	An issue was discovered in mspack/chmd.c in libmspack before 0.7.alpha. There is an off-by-one error in the CHM PMGI/PM

## Risk And Classification

**Problem Types:** CWE-193

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cabextract</a>	<a href="#">Cabextract</a>	All	All	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.0.20060920	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.3	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.4	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.5	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.6	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.0.20060920	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.3	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.4	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.5	alpha	All	All
Application	<a href="#">Cabextract</a>	<a href="#">Libmspack</a>	0.6	alpha	All	All
Application	<a href="#">Cabextract Project</a>	<a href="#">Cabextract</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All

Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	So
#904802 - libmspack: CVE-2018-14679: off-by-one error in CHM PMGI/PMGL chunk number validity checks - Debian Bug report logs	MI
Red Hat Customer Portal	RE
USN-3728-1: libmspack vulnerabilities   Ubuntu security notices	UE
USN-3728-2: ClamAV vulnerabilities   Ubuntu security notices	UE
Clam AntiVirus Memory Errors in 'libmspack' Component Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker	SE
Red Hat Customer Portal	RE
Debian -- Security Information -- DSA-4260-1 libmspack	DE
oss-security - Fw: New cabextract 1.7 and libmspack 0.7 release	MI
cabextract, libmspack: Multiple vulnerabilities (GLSA 201903-20) — Gentoo security	GE
USN-3728-3: ClamAV vulnerabilities   Ubuntu security notices	UE
USN-3789-2: ClamAV vulnerabilities   Ubuntu security notices	UE
[SECURITY] [DLA-1460-1] libmspack security update	ML
Fix off-by-one bounds check on CHM PMGI/PMGL chunk numbers and · kyz/libmspack@72e70a9 · GitHub	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

501043 Alpine Linux Security Update for libmspack

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

751016 OpenSUSE Security Update for libmspack (openSUSE-SU-2021:2802-1)

751043 OpenSUSE Security Update for libmspack (openSUSE-SU-2021:1200-1)

751410 SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2021:3853-1)

751421 SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2021:3859-1)

© [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](#)