Alpine Linux - Bug #9664

Bug # 9662 (Closed): libmspack: Multiple vulnerabilities (CVE-2018-18584, CVE-2018-18585, CVE-2018-18586)

[3.8] libmspack: Multiple vulnerabilities (CVE-2018-18584, CVE-2018-18585, CVE-2018-18586)

11/21/2018 11:31 AM - Alicha CH

Status:	Closed	**Start date:**	11/21/2018
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-18584, CVE-2018-18585, CVE-2018-18586

Description

CVE-2018-18584: A CAB file with a Quantum-compressed block of exactly 38912 bytes will write one byte beyond the end of the input buffer

In mspack/cab.h in libmspack before 0.8alpha and cabextract before 1.8, the CAB
block input buffer is one byte too small for the maximal Quantum block, leading to an out-of-bounds write.

References:

https://www.cabextract.org.uk/libmspack/
https://nvd.nist.gov/vuln/detail/CVE-2018-18584

Patch:

https://github.com/kyz/libmspack/commit/40ef1b4093d77ad3a5cfcee1f5cb6108b3a3bcc2

CVE-2018-18585: CHM files with blank filenames (by having embedded nulls) are allowed, which trips up clients that expect non-blank filenames

chmd_read_headers in mspack/chmd.c in libmspack before 0.8alpha accepts a filename
that has '\0' as its first or second character (such as the "/\0" name).

References:

https://www.cabextract.org.uk/libmspack/
https://nvd.nist.gov/vuln/detail/CVE-2018-18585

Patch:

https://github.com/kyz/libmspack/commit/8759da8db6ec9e866cb8eb143313f397f925bb4f

CVE-2018-18586: chmextract makes no attempt to protect you from relative/absolute paths in CHM filenames

DISPUTED ** chmextract.c in the chmextract sample program, as distributed with libmspack before 0.8alpha, does not protect against absolute/relative pathnames in CHM files, leading to Directory Traversal. NOTE: the vendor disputes that this is a libmspack vulnerability, because chmextract.c was only intended as a source-code example, not a supported application.

References:

https://www.cabextract.org.uk/libmspack/
https://nvd.nist.gov/vuln/detail/CVE-2018-18586

Patch:

https://github.com/kyz/libmspack/commit/7cadd489698be117c47efcadd742651594429e6d

Associated revisions

Revision e59fb237 - 11/27/2018 12:31 PM - Natanael Copa

main/libmspack: security upgrade to 0.8_alpha

CVE-2018-18584, CVE-2018-18585, CVE-2018-18586

fixes #9664

History

#1 - 11/27/2018 12:31 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:e59fb2371eb8b367558761b562b73e8b1935e498.

#2 - 11/28/2018 07:19 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed