

Alpine Linux - Bug #9686

Bug # 9684 (Closed): clamav: Multiple vulnerabilities (CVE-2018-15378, CVE-2018-14680, CVE-2018-14681, CVE-2018-14682)

[3.8] clamav: Multiple vulnerabilities (CVE-2018-15378, CVE-2018-14680, CVE-2018-14681, CVE-2018-14682)

11/26/2018 12:47 PM - Alichu CH

Status:	Closed	Start date:	11/26/2018
Priority:	Normal	Due date:	
Assignee:	Carlo Landmeter	% Done:	100%
Category:	Security	Estimated time:	0.00 hour
Target version:	3.8.2	Security IDs:	CVE-2018-15378, CVE-2018-14680, CVE-2018-14681, CVE-2018-14682
Affected versions:			

Description

Fixes for the following ClamAV vulnerabilities:

CVE-2018-15378: Vulnerability in ClamAV's MEW unpacking feature that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

Fixes for the following vulnerabilities in bundled third-party libraries:

CVE-2018-14680: An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. It does not reject blank CHM filenames.

CVE-2018-14681: An issue was discovered in kwajd_read_headers in mspack/kwajd.c in libmspack before 0.7alpha. Bad KWAJ file header extensions could cause a one or two byte overwrite.

CVE-2018-14682: An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the TOWER macro for CHM decompression.

Fixed In Version:

clamav 0.100.2

References:

<https://github.com/Cisco-Talos/clamav-devel/blob/dev/0.100/NEWS.md#01002>

<http://lists.clamav.net/pipermail/clamav-announce/2018/000033.html>

Associated revisions

Revision b34c6efb - 11/27/2018 03:24 PM - JOWI

main/clamav: security upgrade to 0.100.2

- CVE-2018-15378
- CVE-2018-14680
- CVE-2018-14681
- CVE-2018-14682

fixes #9686

Revision fdb3e21e - 11/27/2018 03:29 PM - JOWI

main/clamav: security upgrade to 0.100.2

- CVE-2018-15378
- CVE-2018-14680
- CVE-2018-14681
- CVE-2018-14682

fixes #9686

History

#1 - 11/27/2018 03:26 PM - Anonymous

- Status changed from New to Resolved
- % Done changed from 0 to 100

Applied in changeset [alpine:b34c6efbc0f5941d4099a372533f14885013e380](#).

#2 - 11/28/2018 07:08 AM - Aicha CH

- Project changed from Alpine Security to Alpine Linux
- Category set to Security
- Status changed from Resolved to Closed