Alpine Linux - Bug #9680

Bug # 9678 (Closed): openjpeg: Multiple vulnerabilities (CVE-2017-17480, CVE-2018-18088)

[3.8] openjpeg: Multiple vulnerabilities (CVE-2017-17480, CVE-2018-18088)

11/22/2018 11:56 AM - Alicha CH

Status:	Closed	**Start date:**	11/22/2018
Priority:	Normal	**Due date:**	
Assignee:	Francesco Colista	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

CVE-2018-18088: NULL pointer dereference in the imagetopnm function of jp2/convert.c

A flaw was found in OpenJPEG 2.3.0. A NULL pointer dereference for "red" in the
imagetopnm function of jp2/convert.c

References:

https://github.com/uclouvain/openjpeg/issues/1152
https://nvd.nist.gov/vuln/detail/CVE-2018-18088

Patch:

https://github.com/uclouvain/openjpeg/commit/cab352e249ed3372dd9355c85e837613fff98fa2

CVE-2017-17480: Stack-buffer overflow in the pgxtovolume function

In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtovolume function in jp3d/convert.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.

References:

https://github.com/uclouvain/openjpeg/issues/1044
https://security-tracker.debian.org/tracker/CVE-2017-17480

Patch:

https://github.com/uclouvain/openjpeg/commit/0bc90e4062a5f9258c91eca018c019b179066c62

Associated revisions

Revision 6dd49eef - 11/22/2018 04:14 PM - Natanael Copa

main/openjpeg: security fixes (CVE-2017-17480,CVE-2018-18088)

also remove unused patches

fixes #9680

History

#1 - 11/22/2018 04:15 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:6dd49eeff4953456d2d668b4e7653967a44a4972.

#2 - 11/26/2018 11:45 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2017-17480, CVE-2018-18088)