Alpine Linux - Bug #9584

Bug # 9582 (Closed): tiff: Multiple vulnerabilities (CVE-2018-10779, CVE-2018-17100, CVE-2018-17101)

[3.8] tiff: Multiple vulnerabilities (CVE-2018-10779, CVE-2018-17100, CVE-2018-17101)

10/25/2018 10:46 AM - Alicha CH

Status:	Closed	**Start date:**	10/25/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

CVE-2018-10779: Heap Buffer Overflow in TIFFWriteScanline of tif_write.c

References:

http://bugzilla.maptools.org/show_bug.cgi?id=2788
https://nvd.nist.gov/vuln/detail/CVE-2018-10779

Patch:

https://gitlab.com/libtiff/libtiff/commit/981e43ecae83935625c86c9118c0778c942c7048

CVE-2018-17100: An issue was discovered in LibTIFF 4.0.9. There is a int32 overflow in multiply_ms in tools/ppm2tiff.c, which can cause a denial of service (crash) or possibly have unspecified other impact via a crafted image file.

References:

http://bugzilla.maptools.org/show_bug.cgi?id=2810

Patch:

https://gitlab.com/libtiff/libtiff/merge_requests/33/diffs?commit_id=6da1fb3f64d43be37e640efbec60400d1f1ac39e

CVE-2018-17101: An issue was discovered in LibTIFF 4.0.9. There are two out-of-bounds writes in cpTags in tools/tiff2bw.c and tools/pal2rgb.c,
which can cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image file.

References:

http://bugzilla.maptools.org/show_bug.cgi?id=2807

Patch:

https://gitlab.com/libtiff/libtiff/merge_requests/33/diffs?commit_id=f1b94e8a3ba49febdd3361c0214a1d1149251577

Associated revisions

Revision 94901081 - 11/06/2018 03:36 PM - Leonardo Arena

main/tiff: security fixes

(CVE-2018-10779, CVE-2018-17100, CVE-2018-17101)

Fixes #9584

History

#1 - 11/06/2018 03:37 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:949010814f11ac10dd7a4b0ccf70090b10aa29bd.

#2 - 11/08/2018 08:34 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-2018-10779, CVE-2018-17100, CVE-2018-17101)