Alpine Linux - Bug #9716

Bug # 9714 (Closed): tiff: Multiple vulnerabilities (CVE-2018-12900, CVE-2018-18557, CVE-2018-18661)

[3.8] tiff: Multiple vulnerabilities (CVE-2018-12900, CVE-2018-18557, CVE-2018-18661)

11/29/2018 10:26 AM - Alicha CH

Status:	Closed	**Start date:**	11/29/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-12900, CVE-2018-18557, CVE-2018-18661

Description

CVE-2018-12900: Heap-based buffer overflow in the cpSeparateBufToContigBuf function resulting in a denial of service

Heap-based buffer overflow in the cpSeparateBufToContigBuf function in tiffcp.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via a crafted TIFF file.

References:

http://bugzilla.maptools.org/show_bug.cgi?id=2798
https://nvd.nist.gov/vuln/detail/CVE-2018-12900

CVE-2018-18557: Out-of-bounds write in tif_jbig.c

LibTIFF 4.0.9 (with JBIG enabled) decodes arbitrarily-sized JBIG into a buffer, ignoring the buffer size, which leads to a tif_jbig.c JBIGDecode out-of-bounds write.

References:

https://bugs.chromium.org/p/project-zero/issues/detail?id=1697
https://nvd.nist.gov/vuln/detail/CVE-2018-18557

CVE-2018-18661: tiff2bw tool failed memory allocation leads to crash

An issue was discovered in LibTIFF 4.0.9. There is a NULL pointer dereference in the function LZWDecode in the file tif_lzw.c.

References:

http://bugzilla.maptools.org/show_bug.cgi?id=2819
https://nvd.nist.gov/vuln/detail/CVE-2018-18661

Patch:

https://gitlab.com/libtiff/libtiff/commit/99b10edde9a0fc28cc0e7b7757aa18ac4c8c225f

Associated revisions

Revision 42e3145e - 12/07/2018 07:26 AM - Natanael Copa

main/tiff: security upgrade to 4.0.10

CVE-2018-12900, CVE-2018-18557, CVE-2018-18661

fixes #9716

History

#1 - 12/07/2018 07:26 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:42e3145e0c57d0a2e3c2717842ae6cfa41e3a03e.

#2 - 12/07/2018 10:47 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed