Alpine Linux - Bug #9444

Bug # 9442 (Closed): lcms2: heap-based buffer overflow in SetData function in cmsIT8LoadFromFile (CVE-2018-16435)

[3.8] lcms2: heap-based buffer overflow in SetData function in cmsIT8LoadFromFile (CVE-2018-16435)

09/21/2018 09:09 AM - Alicha CH

Status:	Closed	**Start date:**	09/21/2018
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:**	

Description

A flaw was found in Little CMS (aka Little Color Management System) 2.9. An integer overflow in the AllocateDataSet function in cmscgats.c, leading to a heap-based buffer overflow in the SetData function via a crafted file in the second argument to cmsIT8LoadFromFile.

References:

https://github.com/mm2/Little-CMS/issues/171
https://nvd.nist.gov/vuln/detail/CVE-2018-16435

Patch:

https://github.com/mm2/Little-CMS/commit/768f70ca405cd3159d990e962d54456773bb8cf8

Associated revisions

Revision 2fabafb2 - 11/06/2018 03:55 PM - Leonardo Arena

main/lcms2: security fix (CVE-2018-16435)

Fixes #9444

History

#1 - 11/06/2018 03:55 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:2fabafb2b32d929a4de15f8ae3e7a8379120e495.

#2 - 11/08/2018 08:43 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-2018-16435)