Alpine Linux - Bug #9798

Bug # 9796 (Closed): openjpeg: Multiple vulnerabilities (CVE-2018-14423, CVE-2018-6616)

[3.8] openjpeg: Multiple vulnerabilities (CVE-2018-14423, CVE-2018-6616)

12/27/2018 07:11 AM - Alicha CH

Status:	Closed	**Start date:**	12/27/2018
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:**	CVE-2018-14423, CVE-2018-6616

Description

CVE-2018-14423: Division-by-zero vulnerabilities in the functions pi_next_pcrl, pi_next_cprl, and pi_next_rpcl in lib/openjp3d/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-14423
https://github.com/uclouvain/openjpeg/issues/1123

Patch:

https://github.com/uclouvain/openjpeg/commit/bd88611ed9ad7144ec4f3de54790cd848175891b

CVE-2018-6616: In OpenJPEG 2.3.0, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-6616
https://github.com/uclouvain/openjpeg/issues/1059

Patch:

https://github.com/hlef/openjpeg/commit/8ee335227bbcaf1614124046aa25e53d67b11ec3

Associated revisions

Revision 12fd347f - 01/01/2019 07:42 AM - Francesco Colista

main/openjpeg: security fixes

- CVE-2018-14423
- CVE-2018-6616

this commit fixes #9798

History

#1 - 01/01/2019 07:42 AM - Francesco Colista

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:12fd347ffe7f9822f46f4cb6f4841ab6fa558edd.

#2 - 01/01/2019 10:27 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed