Alpine Linux - Bug #9522

Bug # 9520 (Closed): libexif: Out-of-bounds heap read in exif_data_save_data_entry function (CVE-2017-7544)

[3.8] libexif: Out-of-bounds heap read in exif_data_save_data_entry function (CVE-2017-7544)

10/08/2018 10:04 AM - Alicha CH

Status:	Closed	**Start date:**	10/08/2018
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

One heap-based out-of-bounds read vulnerabiltiy exists in libexif-0.6.21. When saving the data of an entry tagged with “EXIF_TAG_MAKER_NOTE” to
a buffer and copying the data of the exif entry, there is a mismatch between the computed read size of the entry data and the size of the allocated entry data.
The vulnerability can cause Denial-of-Service, even Information Disclosure (disclosing some critical heap chunk metadata, even other applications’ private data).

References:

https://sourceforge.net/p/libexif/bugs/130/
https://nvd.nist.gov/vuln/detail/CVE-2017-7544

Associated revisions

Revision a9d9f445 - 10/08/2018 01:47 PM - Leonardo Arena

main/libexif: security fix (CVE-2017-7544)

Fixes #9522

History

#1 - 10/08/2018 01:47 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:a9d9f445b7e40ed463fcdb320cd88cde20b3c714.

#2 - 10/09/2018 06:56 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-2017-7544)