Alpine Linux - Bug #6899

Bug # 6898 (Closed): libplist: Multiple issues (CVE-2017-5209, CVE-2017-5545, CVE-2017-5834, CVE-2017-5835, CVE-2017-5836)

[3.6] libplist: Multiple issues (CVE-2017-5209, CVE-2017-5545, CVE-2017-5834, CVE-2017-5835, CVE-2017-5836)

02/20/2017 03:38 PM - Alicha CH

Status:	Closed	**Start date:**	02/20/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.6.1		
Affected versions:		**Security IDs:**	

Description

CVE-2017-5209:

The base64decode function in base64.c in libimobiledevice libplist through 1.12 allows attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read) via split encoded Apple Property List data.

Reference:

https://github.com/libimobiledevice/libplist/issues/84

Patch:

https://github.com/libimobiledevice/libplist/commit/3a55ddd3c4c11ce75a86afbefd085d8d397ff957

CVE-2017-5545:

The main function in plistutil.c in libimobiledevice libplist through 1.12 allows attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read) via Apple Property List data that is too short.

Reference:

https://github.com/libimobiledevice/libplist/issues/87
http://seclists.org/oss-sec/2017/q1/239

Patch:

https://github.com/libimobiledevice/libplist/commit/7391a506352c009fe044dead7baad9e22dd279ee

CVE-2017-5834: heap-buffer-overflow in parse_dict_node

Reference:

https://github.com/libimobiledevice/libplist/issues/89
http://seclists.org/oss-sec/2017/q1/239

Patch:

https://github.com/libimobiledevice/libplist/commit/4765d9a60ca4248a8f89289271ac69cbffcc29bc

CVE-2017-5835: memory allocation error

Reference:

https://github.com/libimobiledevice/libplist/issues/88
http://seclists.org/oss-sec/2017/q1/239

Patch:

https://github.com/libimobiledevice/libplist/commit/26061aac4ec75e7a4469a9aab9a424716223e5c4

CVE-2017-5836: issue in plist_free_data plist.c:185

Reference:

https://github.com/libimobiledevice/libplist/issues/86
http://seclists.org/oss-sec/2017/q1/239

Patch:

https://github.com/libimobiledevice/libplist/commit/7a28a14cf6ed547dfd2e52a4db17f47242bfdef9

Associated revisions

Revision d2b9ac4f - 05/31/2017 02:10 PM - Natanael Copa

community/libplist: security upgrade to 2.0.0

CVE-2017-5209
CVE-2017-5545
CVE-2017-5834
CVE-2017-5835
CVE-2017-5836

This seems to be an update that is ABI compatible, and only kodi uses is.

fixes #6899

History

#1 - 02/21/2017 07:44 AM - Sergei Lukin

Patches are not applicable to libplist 1.12 due to quite significant refactoring of the package since the last release
https://bugzilla.redhat.com/show_bug.cgi?id=1412613#c2

#2 - 05/25/2017 10:39 AM - Natanael Copa

- Target version changed from 3.6.0 to 3.6.1

#3 - 05/31/2017 02:11 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:d2b9ac4f2df9f3cb0899f67bfaf17fc03340d5b6.

#4 - 06/29/2017 07:25 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed