Alpine Linux - Bug #6791

Bug # 6789 (Closed): libarchive: Out of bounds read in lha_read_file_header_1() function (CVE-2017-5601)

[3.5] libarchive: Out of bounds read in lha_read_file_header_1() function (CVE-2017-5601)

02/01/2017 08:06 AM - Alicha CH

Status:	Closed		**Start date:**	02/01/2017
Priority:	Normal		**Due date:**	
Assignee:	Natanael Copa		**% Done:**	100%
Category:	Security		**Estimated time:**	0.00 hour
Target version:	3.5.2			
Affected versions:			**Security IDs:**	

Description

The vulnerability is caused due to an error in the
"lha_read_file_header_1()" function
(archive_read_support_format_lha.c), which can be exploited to trigger
an out-of-bounds read memory access via a specially crafted archive.

Affected versions:

libarchive version 3.2.2.
Other versions may also be affected.

Reference:

https://secunia.com/secunia_research/2017-3/

Patch:

https://github.com/libarchive/libarchive/commit/98dcbbf0bf4854bf987557e55e55fff7abbf3ea9

Associated revisions

Revision 238237da - 02/01/2017 01:19 PM - Sergei Lukin

main/libarchive: security fixes #6791

CVE-2017-5601: Out of bounds read in lha_read_file_header_1() function

History

#1 - 02/01/2017 01:25 PM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:238237daad198ce03edca610ca2b5876ecdcc0b9.

#2 - 02/02/2017 09:26 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed