Alpine Linux - Bug #7362

Bug # 7360 (Closed): openldap: Double free vulnerability in servers/slapd/back-mdb/search.c (CVE-2017-9287)

[3.6] openldap: Double free vulnerability in servers/slapd/back-mdb/search.c (CVE-2017-9287)

06/01/2017 10:52 AM - Alicha CH

Status:	Closed	**Start date:**	06/01/2017
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

servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the
directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.

Reference:

https://nvd.nist.gov/vuln/detail/CVE-2017-9287

Patch:

https://www.openldap.org/devel/gitweb.cgi?p=openldap.git;a=commit;h=0cee1ffb6021b1aae3fcc9581699da1c85a6dd6e

Associated revisions

Revision 70711fe4 - 06/01/2017 11:14 AM - Natanael Copa

main/openldap: sec fix for CVE-2017-9287

fixes #7362

History

#1 - 06/01/2017 12:02 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:70711fe484191a3cb0f1fded665524c40f4d51dc.

#2 - 06/15/2017 10:43 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed