Alpine Linux - Bug #7328

Bug # 7326 (Closed): libtasn1: asn1_find_node() based stackoverflow (CVE-2017-6891)

[3.6] libtasn1: asn1_find_node() based stackoverflow (CVE-2017-6891)

05/25/2017 11:10 AM - Alicha CH

Status:	Closed	**Start date:**	05/25/2017
Priority:	Normal	**Due date:**	
Assignee:	Francesco Colista	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.6.1		
Affected versions:		**Security IDs:**	

Description

Two errors in the "asn1_find_node()" function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be exploited to cause a stacked-based
buffer overflow by tricking a user into processing a specially crafted assignments file via the e.g. asn1Coding utility.

References:

https://secuniaresearch.flexerasoftware.com/secunia_research/2017-11/
https://nvd.nist.gov/vuln/detail/CVE-2017-6891

Patch:

http://git.savannah.gnu.org/gitweb/?p=libtasn1.git;a=commit;h=5520704d075802df25ce4ffccc010ba1641bd484

Associated revisions

Revision 9c7bef12 - 05/25/2017 01:33 PM - Francesco Colista

main/libtasn1: security fix for CVE-2017-6891. Fixes #7328

History

#1 - 05/25/2017 02:02 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:9c7bef126531b81cd07fa8fb09f8fde105afe6ca.

#2 - 05/25/2017 02:06 PM - Francesco Colista

- Category set to Security

- Status changed from Resolved to Closed

- Assignee changed from Natanael Copa to Francesco Colista