Alpine Linux - Bug #7432

Bug # 7431 (Closed): libgcrypt: Possible timing attack on EdDSA session key (CVE-2017-9526)

[3.6] libgcrypt: Possible timing attack on EdDSA session key (CVE-2017-9526)

06/15/2017 03:29 PM - Alicha CH

Status:	Closed	**Start date:**	06/15/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.6.2		
Affected versions:		**Security IDs:**	

Description

An attacker who learns the EdDSA session key from side-channel observation during the signing process, can easily recover the long-term secret key. Storing the session key in secure memory ensures that constant time point operations are used in the MPI library.

Fixed In Version:

libgcrypt 1.7.7

Reference:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9526

Patches:

1.7.x: https://git.gnupg.org/cgi-bin/gitweb.cgi?p=libgcrypt.git;a=commit;h=f9494b3f258e01b6af8bd3941ce436bcc00afc56
Curve Ed25519 signing and verification inplemented in 1.6.0 with
https://git.gnupg.org/cgi-bin/gitweb.cgi?p=libgcrypt.git;a=commit;h=bc5199a02abe428ad377443280b3eda60141a1d6
and following refactorings.

Associated revisions

Revision b95bfcc9 - 06/16/2017 12:30 PM - Natanael Copa

main/libgcrypt: security upgrade to 1.7.7 (CVE-2017-9526)

fixes #7432

History

#1 - 06/16/2017 01:41 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:b95bfcc998819366a8cadce0f079feda32c8c2ab.

#2 - 07/05/2017 08:28 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed