Alpine Linux - Bug #7347

Bug # 7346 (Closed): strongswan: Multiple vulnerabilities (CVE-2017-9022, CVE-2017-9023)

[3.6] strongswan: Multiple vulnerabilities (CVE-2017-9022, CVE-2017-9023)

05/31/2017 09:49 AM - Alicha CH

Status:	Closed	**Start date:**	05/31/2017
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-2017-9022: Insufficient validation of RSA public keys passed to the gmp plugin

RSA public keys passed to the gmp plugin aren't validated sufficiently before attempting signature verification, so that invalid input might lead to a floating point
exception and crash of the process. A certificate with an appropriately prepared public key sent by a peer could be used for a denial-of-service attack.

Affected versions:

All versions since 4.4.0, up to and including 5.5.2.

Fixed In Version:

strongswan 5.5.3

References:

https://www.strongswan.org/blog/2017/05/30/strongswan-vulnerability-(cve-2017-9022).html

Patches:

https://download.strongswan.org/security/CVE-2017-9022/

CVE-2017-9023: Incorrect Handling of CHOICE types in ASN.1 parser and x509 plugin

ASN.1 CHOICE types are not correctly handled by the ASN.1 parser when parsing X.509 certificates with extensions that use such types.
This could lead to infinite looping of the thread parsing a specifically crafted certificate.

Affected versions:

All strongSwan versions up to and including 5.5.2

Fixed In Version:

strongswan 5.5.3

References:

https://www.strongswan.org/blog/2017/05/30/strongswan-vulnerability-(cve-2017-9023).html

Patches:

https://download.strongswan.org/security/CVE-2017-9023/

Associated revisions

Revision f647e2d3 - 05/31/2017 10:36 AM - Natanael Copa

main/strongswan: security upgrade to 5.5.3 (CVE-2017-9022,CVE-2017-9023)

fixes #7347

History

#1 - 05/31/2017 10:37 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:f647e2d3d31f6c5e3c4f4f41bfbee7eea8d02271.

#2 - 06/15/2017 03:34 PM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed