Alpine Linux - Bug #9484

Bug # 9482 (Closed): strongswan: Multiple vulnerabilities (CVE-2018-16151, CVE-2018-16152)

[3.8] strongswan: Multiple vulnerabilities (CVE-2018-16151, CVE-2018-16152)

09/27/2018 08:57 AM - Alicha CH

Status:	Closed	**Start date:**	09/27/2018
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

CVE-2018-16151: In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0,
the RSA implementation based on GMP does not reject excess data after the encoded algorithm OID during PKCS#1 v1.5 signature verification.
Similar to the flaw in the same version of strongSwan regarding digestAlgorithm.parameters, a remote attacker can forge signatures when small
public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication.

References:

https://www.strongswan.org/blog/2018/09/24/strongswan-vulnerability-(cve-2018-16151,-cve-2018-16152).html
https://nvd.nist.gov/vuln/detail/CVE-2018-16151

Patches:

https://download.strongswan.org/patches/27_gmp_pkcs1_verify_patch/strongswan-5.3.1-5.6.0_gmp-pkcs1-verify.patch
https://download.strongswan.org/patches/27_gmp_pkcs1_verify_patch/strongswan-5.6.1-5.6.3_gmp-pkcs1-verify.patch

CVE-2018-16152: In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0,
the RSA implementation based on GMP does not reject excess data in the digestAlgorithm.parameters field during PKCS#1 v1.5 signature
verification. Consequently, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication.

References:

https://www.strongswan.org/blog/2018/09/24/strongswan-vulnerability-(cve-2018-16151,-cve-2018-16152).html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-16152

Patches:

https://download.strongswan.org/patches/27_gmp_pkcs1_verify_patch/strongswan-5.3.1-5.6.0_gmp-pkcs1-verify.patch
https://download.strongswan.org/patches/27_gmp_pkcs1_verify_patch/strongswan-5.6.1-5.6.3_gmp-pkcs1-verify.patch

Associated revisions

Revision 142cd066 - 10/02/2018 12:20 PM - Natanael Copa

main/strongswan: backport security fix (CVE-2018-16151, CVE-2018-16152)

fixes #9484

History

#1 - 10/02/2018 12:21 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:142cd0660c759d91ccdd0b6b6fd5f4959413ed93.

#2 - 10/04/2018 10:10 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-16151, CVE-2018-16152)