CVE-2018-16152

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16152
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-26 21:29:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	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 F

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Strongswan	Strongswan	All	All	All	All
Application	Strongswan	Strongswan	All	All	All	All
Application	Strongswan	Strongswan	All	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2019:2598-1: important: Security update	SUSE	lists.opensuse.org	

strongSwan - strongSwan Vulnerability (CVE-2018-16151, CVE-2018-16152)		www.strongswan.org	
[security-announce] openSUSE-SU-2019:2594-1: important: Security update	SUSE	lists.opensuse.org	
strongSwan: Multiple vulnerabilities (GLSA 201811-16) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
[SECURITY] [DLA 1522-1] strongswan security update	MLIST	lists.debian.org	Mailing List, Third Party
USN-3771-1: strongSwan vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Advisory
Debian -- Security Information -- DSA-4305-1 strongswan	DEBIAN	www.debian.org	Third Party Advisory
strongSwan - strongSwan Vulnerability (CVE-2018-16151, CVE-2018-16152)	CONFIRM	www.strongswan.org	Mitigation, Patch, Techn
[security-announce] openSUSE-SU-2020:0403-1: moderate: Security update f	SUSE	lists.opensuse.org	
strongSwan - strongSwan Vulnerability (CVE-2018-16151, CVE-2018-16152)	MITRE	www.strongswan.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 500667 Alpine Linux Security Update for strongswan
- 504437 Alpine Linux Security Update for strongswan
- 710305 Gentoo Linux strongSwan Multiple Vulnerabilities (GLSA 201811-16)
- 753457 SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:14887-1)