CVE-2018-15836

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-15836
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-26 21:29:00 UTC
Updated	2019-01-10 17:52:00 UTC
Description	In verify_signed_hash() in lib/liboswkeys/signatures.c in Openswan before 2.6.50.1, the RSA implementation does not verif

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xelerance	Openswan	All	All	All	All
Application	Xelerance	Openswan	All	All	All	All

References

Reference	Source	Link	Ta
Update VERSION to 2.6.50.1 · xelerance/Openswan@0b460be · GitHub	CONFIRM	github.com	P
[Openswan Users] Xelerance has released Openswan 2.6.50.1	MLIST	lists.openswan.org	R
wo#7449 . verify padding contents for IKEv2 RSA sig check · xelerance/Openswan@9eaa6c2 · GitHub	CONFIRM	github.com	P
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report