



# CVE-2018-15836

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

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

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Xelerance</a>	<a href="#">Openswan</a>	All	All	All	All
Application	<a href="#">Xelerance</a>	<a href="#">Openswan</a>	All	All	All	All

## References

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

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**