



# CVE-2018-16253

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

## Summary

<b>CVE</b>	CVE-2018-16253
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-07 20:29:00 UTC
<b>Updated</b>	2018-12-13 18:06:00 UTC
<b>Description</b>	In sig_verify() in x509.c in axTLS version 2.1.3 and before, the PKCS#1 v1.5 signature verification does not properly verify t

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
axTLS Embedded SSL / Re: [axtls-general] Problems of PKCS#1 v1.5 RSA Signature Verification	MLIST	<a href="#">sourceforge.net</a>	Exploit, TH
Apply CVE fixes for X509 parsing · igrr/axtls-8266@5efe294 · GitHub	CONFIRM	<a href="#">github.com</a>	Patch, Thi
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

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

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](#)**