CVE-2018-16149

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16149
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-07 20:29:00 UTC
Updated	2019-01-31 15:04:00 UTC
Description	In sig_verify() in x509.c in axTLS version 2.1.3 and before, the PKCS#1 v1.5 signature verification blindly trusts the declare

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axtls Project	Axtls	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	sourceforge.net	Exploit, Pa
Apply CVE fixes for X509 parsing · igrr/axtls-8266@5efe294 · GitHub	CONFIRM	github.com	Patch, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

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