CVE-2016-10213

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-10213
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-08 16:59:00 UTC
Updated	2017-03-01 14:02:00 UTC
Description	A10 AX1030 and possibly other devices with software before 2.7.2-P8 uses random GCM nonce generations, which makes

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	A10networks	Advanced Core Operating System	All	p7	All	All

References

Reference	Source	Link
GitHub - nonce-disrespect/nonce-disrespect: Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS	MISC	gith
CVE-2016-0270 GCM nonce vulnerability	CONFIRM	www
A10 Networks AX1030 CVE-2016-10213 Information Disclosure Vulnerability	BID	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

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