



# CVE-2016-10213

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

## Summary

<b>CVE</b>	CVE-2016-10213
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-02-08 16:59:00 UTC
<b>Updated</b>	2017-03-01 14:02:00 UTC
<b>Description</b>	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	<a href="#">gith</a>
CVE-2016-0270 GCM nonce vulnerability	CONFIRM	<a href="#">ww</a>
A10 Networks AX1030 CVE-2016-10213 Information Disclosure Vulnerability	BID	<a href="#">ww</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nvd</a>

No vendor comments have been submitted for this CVE.

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

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](#)**