



CVE-2017-5933

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-5933
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-08 16:59:00 UTC
Updated	2017-03-14 19:27:00 UTC
Description	Citrix NetScaler ADC and NetScaler Gateway 10.5 before Build 65.11, 11.0 before Build 69.12/69.123, and 11.1 before Bui

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Netscaler Application Delivery Controller Firmware	All	All	All	All
Application	Citrix	Netscaler Application Delivery Controller Firmware	All	All	All	All
Application	Citrix	Netscaler Application Delivery Controller Firmware	All	All	All	All

References

Reference	Source	Link
GitHub - nonce-disrespect/nonce-disrespect: Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS	MISC	gith
Vulnerability in Citrix NetScaler Application Delivery Controller and NetScaler Gateway GCM nonce generation	CONFIRM	sup
Citrix NetScaler Application Delivery Controller and Gateway Information Disclosure Vulnerability	BID	ww
CVE Program record	CVE.ORG	ww
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](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)