



CVE-2017-17382

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

Summary

CVE	CVE-2017-17382
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-13 16:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway 10.5 before build 67.13, 11.0 before build 71

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Citrix	Application Delivery Controller Firmware	10.5	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	11.0	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	11.1	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	12.0	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	10.5	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	11.0	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	11.1	All	All	All
Operating System	Citrix	Application Delivery Controller Firmware	12.0	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	10.5	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	11.0	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	11.1	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	12.0	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	10.5	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	11.0	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	11.1	All	All	All
Operating System	Citrix	Netscaler Gateway Firmware	12.0	All	All	All

References	
Reference	Source
Citrix NetScaler TLS Side Channel Leakage Flaw Lets Remote Users Decrypt TLS Session Data - SecurityTracker	SecurityTracker
TLS Padding Oracle Vulnerability in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway	Citrix
Multiple Citrix Products CVE-2017-17382 Information Disclosure Vulnerability	Bleichenbacher
The ROBOT Attack - Return of Bleichenbacher's Oracle Threat	MitRE
VU#144389 - TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding	CVE
CVE Program record	CVE
NVD vulnerability detail	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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)