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

No vendor comments have been submitted for this CVE.

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