NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967

Title
NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967

CTX Number
CTX579459

Article Type
Security Bulletin

Created Date
10/Oct/2023

Last Modified Date
15/Jul/2024

Severity
Critical

Status
Final

Details
Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway).

Affected Versions:

The following supported versions of NetScaler ADC and NetScaler Gateway are affected by the vulnerabilities:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19
- NetScaler ADC 13.1-FIPS before 13.1-37.164
- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End-of-Life (EOL) and is vulnerable.

This bulletin only applies to customer-managed NetScaler ADC and NetScaler Gateway products. Customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

Summary:

NetScaler ADC and NetScaler Gateway contain unauthenticated buffer-related vulnerabilities mentioned below

CVE ID	Description	Pre-requisites	CWE
CVE-2023-4966	Sensitive information disclosure	Application must be configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	CWE-119
CVE-2023-4967	Denial of service	Appliance must be configured as a Gateway (VPN virtual	CWE-119

		server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	

Mitigating Factors

None.

Instructions

Exploits of CVE-2023-4966 on unmitigated appliances have been observed. Cloud Software Group strongly urges customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible:

- NetScaler ADC and NetScaler Gateway 14.1-8.50 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-49.15 and later releases of 13.1
- NetScaler ADC and NetScaler Gateway 13.0-92.19 and later releases of 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.164 and later releases of 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.300 and later releases of 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.300 and later releases of 12.1-NDcPP

Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End-of-Life (EOL). Customers are recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities.

Cloud Software Group has published a related blog at https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/ which contains further context.

Cloud Software Group has published an additional blog at https://www.netscaler.com/blog/news/netscaler-investigation-recommendations-for-cve-2023-4966/ which contains recommendations for investigation of this vulnerability.

Citrix Support

What Citrix is Doing

Citrix is notifying customers and channel partners about this potential security issue through the publication of this security bulletin on the Citrix Knowledge Center at https://support.citrix.com/securitybulletins.

Obtaining Support on This Issue

If you require technical assistance with this issue, please contact Citrix Technical Support. Contact details for Citrix Technical Support are available at https://www.citrix.com/support/open-a-support-case .

Subscribe to Receive Alerts

Citrix strongly recommends that all customers subscribe to receive alerts when a Citrix security bulletin is created or modified at https://support.citrix.com/user/alerts.

Reporting Security Vulnerabilities to Citrix

Citrix welcomes input regarding the security of its products and considers any and all potential vulnerabilities seriously. For details on our vulnerability response process and guidance on how to report security-related issues to Citrix, please see the following webpage: https://www.citrix.com/about/trust-center/vulnerability-process.html .

Disclaimer

This document is provided on an "as is" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Your use of the information on the document is at your own risk. Citrix reserves the

right to change or update this document at any time. Customers are therefore recommended to always view the latest version of this document directly from the Citrix Knowledge Center.

Additional Resources

2023-10-10 T 16:00:00Z	Initial Publication
2023-10-17 T 16:00:00Z	Inclusion of information related to the exploitation of CVE-2023-4966
2023-10-23 T 16:00:00Z	Inclusion of a link to the Cloud Software Group blog post about CVE-2023-4966
2023-11-20 T 17:00:00Z	Inclusion of a link to an additional Cloud Software Group blog post about CVE-2023-4966
2023-11-27 T 17:00:00Z	Correction to article workflow to enable customer email alerts
2024-07-15 T 15:30:00Z	Platform migration

NetScaler | Netscaler Gateway

Was this article helpful? ★ ★ ★ ★ ★