NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777

Article Record Type : Security Bulletin

Article Id : CTX693420

Created Date : 06-10-2025 18:19

Last Modified Date : 06-17-2025 13:48

Summary

Severity - Critical

Description of Problem

A vulnerability has been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway). Refer below for further details.

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 14.1-43.56
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP
- NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS

Note: NetScaler ADC and NetScaler Gateway versions 12.1 and 13.0 are now End Of Life (EOL) and are vulnerable. Customers are recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities.

Additional Note: Secure Private Access on-prem or Secure Private Access Hybrid deployments using NetScaler instances are also affected by the vulnerabilities. Customers need to upgrade these NetScaler instances to the recommended NetScaler builds to address the vulnerabilities.

This bulletin only applies to customer-managed NetScaler ADC and NetScaler Gateway. Cloud Software Group upgrades the Citrix-managed cloud services and Citrix-managed Adaptive Authentication with the necessary software updates.

Details

NetScaler ADC and NetScaler Gateway contain the vulnerabilities mentioned below:

CVE ID	Description	Pre-conditions	CWE	CVSSv4
CVE-2025-5349	Improper access control on the NetScaler Management Interface	Access to NSIP, Cluster Management IP or local GSLB Site IP	CWE-284: Improper Access Control	CVSS v4.0 Base Score: 8.7 (CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L)

Live Support

CVE-2025-5777	Insufficient input validation leading to memory overread	NetScaler must be configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	CWE-125: Out-of-bounds Read	CVSS v4.0 Base Score: 9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L)

What Customers Should Do

Cloud Software Group strongly urges affected customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions as soon as possible.

- NetScaler ADC and NetScaler Gateway 14.1-43.56 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-58.32 and later releases of 13.1
- NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.235 and later releases of 13.1-FIPS and 13.1-NDcPP
- NetScaler ADC 12.1-FIPS 12.1-55.328 and later releases of 12.1-FIPS

Additionally, we recommend running the following commands to terminate all active ICA and PCoIP sessions after all NetScaler appliances in the HA pair or cluster have been upgraded to the fixed builds.:

```
kill icaconnection -all

kill pcoipConnection -all
```

Please ensure that the formatting remains intact as you copy and paste these commands.

Note: NetScaler ADC and NetScaler Gateway versions 12.1 and 13.0 are now End Of Life (EOL) and no longer supported. Customers are recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities.

Acknowledgements

Cloud Software Group thanks Positive Technologies and ITA MOD CERT (CERTDIFESA) for working with us to protect Cloud Software Group customers.

Additional information / Reference

Changelog

2025-06-17	Initial Publication

Disclaimer

The information on this page is being provided to you on an "AS IS" and "AS-AVAILABLE" basis. The issues described on this page may or may not impact your system(s). Cloud Software Group, Inc. and its subsidiaries (collectively, "Cloud SG") make no representations, warranties, or guarantees as to the information contained herein. ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. BY ACCESSING THIS PAGE, YOU ACKNOWLEDGE THAT CLOUD SG SHALL IN NO EVENT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE CONSEQUENTIAL DAMAGES THAT ARISE OUT OF YOUR USE OR FAILURE TO USE THE INFORM, CONTAINED HEREIN. Cloud SG reserves the right to change or update the information on this page at any time.

Live Support

We accordingly recommend that you always view the latest version of this page. The information contained herein is being provided to you under the terms of your applicable customer agreement with Cloud SG, and may be used only for the purposes contemplated by such agreement. If you do not have such an agreement with Cloud SG, this information is provided under the cloud.com Terms of Use, and may be used only for the purposes contemplated by such Terms of Use.

FOLLOW CITRIX

cloud SOFTWARE GROUP

Legal | Do Not Sell My Personal Information | Cookie Preferences

© 2025 Cloud Software Group, Inc. All rights reserved

Live Support