Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

July 20, 2023 TLP:CLEAR Report: 202307201700

Patch for Critical and High NetScaler ADC (Citrix ADC) and NetScaler Gateway (Citrix Gateway) Vulnerabilities

Executive Summary

On July 18, 2023, Citrix published a security bulletin for NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway). The bulletin regards a patch for three vulnerabilities—one rated 'Critical' and two rated 'High'—that Citrix is encouraging all affected users to implement immediately.

HC3 has noticed activity regarding at least one of these vulnerabilities on the dark web, and highly recommends all public and private health sector organizations to identify all instances of NetScaler ADC and NetScaler Gateway on their network, and deploy the patch as soon as possible.

Report

NetScaler ADC (Citrix ADC) is an application delivery controller that performs application-specific traffic analysis to intelligently distribute, optimize, and secure Layer 4 to Layer 7 network traffic for web applications.

NetScaler Gateway (Citrix Gateway) consolidates remote access infrastructure to provide single sign-on across all applications, whether in a data center, in a cloud, or if the apps are delivered as SaaS apps. It allows people to access any app, from any device, through a single URL.

Affected Versions

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

- NetScaler ADC and NetScaler Gateway 13.1 (before 13.1-49.13)
- NetScaler ADC and NetScaler Gateway 13.0 (before 13.0-91.13)
- NetScaler ADC 13.1-FIPS (before 13.1-37.159)
- NetScaler ADC 12.1-FIPS (before 12.1-55.297)
- NetScaler ADC 12.1-NDcPP (before 12.1-55.297)

Vulnerabilities

CVE ID	Affected Products	Description	About	CWE	CVSS
CVE-2023-3466	Citrix ADC, Citrix Gateway	Reflected Cross-Site Scripting (XSS)	Pre-requisites: Requires victim to access an attacker-controlled link in the browser while being on a network with connectivity to the NSIP	CWE-20	8.3
CVE-2023-3467	Citrix ADC, Citrix Gateway	Privilege Escalation to root administrator (nsroot)	Pre-requisites: Authenticated access to NSIP or SNIP with management interface access	CWE-269	8
CVE-2023-3519	Citrix ADC, Citrix Gateway	Unauthenticated remote code execution	Pre-requisites: Appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	CWE-94	9.8

CVE ID	Affected Products	Description	About	CWE	CVSS
			A remote, unauthenticated attacker can exploit this vulnerability to execute arbitrary code on a vulnerable server. For a target appliance to be vulnerable to exploitation, it must be configured as a Gateway (e.g. VPN, ICA Proxy, CVP, RDP Proxy) or an AAA virtual server. The vulnerability is rated as critical and Citrix reports that "Exploits of CVE-2023-3519 on unmitigated appliances have been observed."		

Patches, Mitigations, and Workarounds

Currently, exploits of CVE-2023-3519 on unmitigated appliances have been observed. Customers of NetScaler ADC and NetScaler Gateway are strongly encouraged to install relevant updated versions as soon as possible.

- NetScaler ADC and NetScaler Gateway (13.1-49.13 and later releases)
- NetScaler ADC and NetScaler Gateway (13.0-91.13 and later releases of 13.0)
- NetScaler ADC 13.1-FIPS (13.1-37.159 and later releases of 13.1-FIPS)
- NetScaler ADC 12.1-FIPS (12.1-55.297 and later releases of 12.1-FIPS)
- NetScaler ADC 12.1-NDcPP (12.1-55.297 and later releases of 12.1-NDcPP)

Citrix also made two additional notes regarding affected versions and mitigations:

1) NetScaler ADC and NetScaler Gateway version 12.1, which are End Of Life (EOL), are vulnerable and customers using these versions recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities.
2) The bulletin only applies to customer-managed NetScaler ADC and NetScaler Gateway—customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

References

Citrix ADC
https://developer.cloud.com/app-delivery-and-security/citrix-adc/docs/overview

Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467
https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Citrix Gateway
https://docs.citrix.com/en-us/citrix-gateway.html#:~:text=Citrix%20Gateway%20consolidates%20remote%20access,device%2C%20through%20a%20single%20URL.

CVE-2023-3519: Critical RCE in Netscaler ADC (Citrix ADC) and Netscaler Gateway (Citrix Gateway)
https://www.tenable.com/blog/cve-2023-3519-critical-rce-in-netscaler-adc-citrix-adc-and-netscaler-gateway-citrix-gateway

Zero-Day Attacks Exploited Critical Vulnerability in Citrix ADC and Gateway
https://thehackernews.com/2023/07/zero-day-attacks-exploited-critical.html

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback