Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

November 30, 2023 TLP:CLEAR Report: 202311301200

Citrix Bleed Vulnerability

Executive Summary

On October 10, 2023, Citrix released a security advisory for a vulnerability that impacts the NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway). This vulnerability is tracked as CVE-2023-4966 and has also been referred to as 'Citrix Bleed'. The Citrix Bleed vulnerability is being actively exploited, and HC3 strongly urges organizations to upgrade to prevent further damage against the Healthcare and Public Health (HPH) sector. This alert contains information on attack detection and mitigation of the vulnerability. The following versions are currently capable of being exploited:

- 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 and NetScaler Gateway version 12.1 (EOL)
- NetScaler ADC 13.1FIPS before 13.1-37.163
- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

It should also be noted that NetScaler ADC and NetScaler Gateway version 12.1 are now considered End-of-Life and will also be vulnerable to CVE-2023-4966.

Patches, Mitigations, and Workarounds

Citrix released a patch for this vulnerability in early October, but it has been reported that the vulnerability was being exploited as a zero-day since August 2023. The manufactor has also warned that these compromised sessions will still be active after a patch has been implemented. HC3 encourages all administrators to follow Citrix's guidance to upgrade their devices and remove any active or persistent sessions with the following commands:

- kill aaa session -all
- kill icaconnection -all
- kill rdp connection -all
- kill pcoipConnection -all
- clear lb persistentSessions

Additional recommended actions for investigating any potential exploits of CVE-2023-4966 are provided by NetScaler here, and further technical details, threat actor activity, and indicators of compromise from CISA can be obtained here and here. HC3 strongly encourages users and administrators to review these recommended actions and upgrade their devices to prevent serious damage to the HPH sector.

References

CISA Guidance for Addressing Citrix NetScaler ADC and Gateway Vulnerability CVE-2023-4966, Citrix Bleed
https://www.cisa.gov/guidance-addressing-citrix-netscaler-adc-and-gateway-vulnerability-cve-2023-4966-citrix-bleed

#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

CVE-2023-4966: Critical security update now available for NetScaler ADC and NetScaler Gateway
https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/

NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967
https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

CVE-2023-4966 Detail
https://nvd.nist.gov/vuln/detail/CVE-2023-4966

Contact Information

If you have any additional questions, or wish to subscribe to HC3 alerts and webinars, contact us at HC3@HHS.GOV. All HC3 materials can be found at WWW.HHS.GOV/HC3.

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