Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

November 22, 2023 TLP:CLEAR Report: 202311221200

Lockbit 3.0 Exploiting Citrix Bleed Vulnerability

Executive Summary

On October 10, 2023, Citrix released a security advisory for a vulnerability that impacts 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’. A recent joint Cybersecurity Advisory from multiple agencies, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), have highlighted that the Lockbit 3.0 Ransomware-as-a-Service group has been actively exploiting this vulnerability. Lockbit 3.0 has previously conducted operations against varying organizations, including those in the Healthcare and Public Health (HPH) sector. HC3 strongly urges users to upgrade their devices to prevent further damage against the HPH sector.

Report

On November 21, 2023, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Multi-State Information Sharing & Analysis Center (MS-ISAC), and the Australian Signals Directorate’s Australian Cyber Security Center (ASD’s ACSC) released a joint Cybersecurity Advisory highlighting Lockbit 3.0’s activity, and their exploitation of the Citrix Bleed vulnerability, which is tracked as CVE-2023-4966. This flaw is a buffer overflow vulnerability that exists within the Citrix NetScaler ADC and NetScaler appliances. The exploitation of this vulnerability can allow a threat actor to bypass multi-factor authentication (MFA) and hijack legitimate user sessions.

Once the attacker has obtained access to valid cookies, the threat actor is able to create an authenticated session within the appliance without requiring a username, password, or access to MFA tokens. This is acquired by the actor sending an HTTP GET request with a crafted HTTP Host Header, which results in the vulnerable appliance returning system memory information, and the returned information containing a valid NetScaler AAA session cookie. 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 can be viewed here, and further technical details, threat actor activity, and indicators of compromise from CISA can be obtained 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

#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, 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