CYBER FLASH

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Canadian Centre for Cyber Security (Cyber Centre) is aware of exploitation of Canadian victims via a zero-day vulnerability in Citrix Netscaler ADC and Netscaler Gateway (CVE-2023-4966). On October 10, 2023, Citrix released a patch and a security bulletin to address this vulnerability [1]. The Cyber Centre also released an advisory on October 10, 2023, to highlight the Citrix bulletin with a recommendation for system owners to apply the necessary updates [2].

Technical Details

On October 28, 2023, the Cyber Centre was made aware of a Canadian organization that was compromised via CVE-2023-4966, a zero-day vulnerability in Citrix Netscaler ADC and Netscaler

Gateway. Analysis indicated that the compromise occurred as a zero-day exploitation event prior to Citrix releasing a patch.

It was determined that a vulnerability in the OpenID Connect Discovery endpoint allowed for an unauthenticated actor to perform a buffer over-read. The data returned by this buffer over-read included session tokens that were subsequently used to authenticate to the device [3].

Access to the virtual desktop via the extracted token resulted in the execution of discovery commands, the dropping of malicious payloads, staging of files for exfiltration, and retrieval of data from the domain controller.

The Cyber Centre strongly recommends that:

- Organizations review the Citrix security advisory [1] and apply the necessary updates.
- Any organizations using Citrix Netscaler ADC and Netscaler Gateway should review the NetScaler blog post [5] for details on resetting session tokens, even if updates have been applied.
- Organizations review and implement the Cyber Centre's Top 10 IT Security Actions [6] with an emphasis on the following topics:
    - Consolidating, monitoring, and defending Internet gateways.
    - Patching operating systems and applications.
    - Segmenting and separating information.
    - Protecting information at the enterprise level.
    - Isolating web-facing applications.
    - Implement application allow lists.

The Cyber Centre wishes to emphasize that zero-day exploitation has been observed, and mitigation efforts resulting from the compromise of systems by competent threat actors may require more than simply mitigating individual issues, systems, and servers. The Cyber Centre recommends affected customers review the Cyber Centre joint cybersecurity advisory on technical approaches to uncovering and remediating malicious activity [7].

References

Information provided by organizations not subject to the Official Languages Act is in the language(s) provided.

[1] 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

[2] - Citrix security advisory

https://www.cyber.gc.ca/en/alerts-advisories/citrix-security-advisory-av23-614

[3] Citrix Bleed: Leaking Session Tokens with CVE-2023-4966

https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966

[4] MITRE ATT&K

https://attack.mitre.org/

[5] 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/

[6] Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)

https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089

[7] Joint cybersecurity advisory - Technical approaches to uncovering and remediating malicious activity.

https://www.cyber.gc.ca/en/news-events/joint-cybersecurity-advisory

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts