MANDIANT
NOW PART OF Google Cloud

Citrix NetScaler ADC/Gateway: CVE-2023-4966 Remediation

1.2 – October 24, 2023

CHANGE LOG

Version – Date	**Notes**
1.0 – October 17, 2023	Initial document
1.1 – October 19, 2023	Added additional commands to execute post update)
1.2 – October 24, 2023	Added an additional indicator within the Detection section

This is a work-in progress document and will be updated as new information for remediation actions are identified.

Background

On October 10, 2023, Citrix released a security bulletin for a sensitive information disclosure vulnerability (CVE-2023-4966) impacting NetScaler ADC and NetScaler Gateway appliances.

Mandiant has identified zero-day exploitation of this vulnerability in the wild beginning in late August 2023. Successful exploitation could result in the ability to hijack existing authenticated sessions, therefore bypassing multifactor authentication (MFA) or other strong authentication requirements. These sessions may persist after the update to mitigate CVE-2023-4966 has been deployed. Additionally, prior to the update being deployed, we have observed session hijacking where session data was stolen and subsequently used by a threat actor.

The authenticated session hijacking could then result in further downstream access based upon the permissions and scope of access that the identity or session was permitted. A threat actor could utilize this method to harvest additional credentials, laterally pivot, and gain access to additional resources within an environment.
To date, Mandiant has observed exploitation at professional services, technology, and government organizations.

Based upon these observations, Mandiant is providing additional steps for remediating and reducing risks related to this vulnerability.

The following versions of NetScaler ADC and Gateway appliances are impacted by the vulnerability:

- 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 13.1-FIPS before 13.1-37.164
- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

  Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End-of-Life (EOL) and is also vulnerable.

Citrix has noted that Customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication are not impacted by CVE-2023-4966.

Remediation

- Isolate NetScaler ADC and Gateway appliances for testing and preparation of patch deployment.

  Note: If the vulnerable appliances cannot be prioritized for patching, Mandiant recommends that the appliances have ingress IP address restrictions enforced to limit the exposure and attack surface until the necessary patches have been applied.

- Upgrade vulnerable NetScaler ADC and Gateway appliances to the latest firmware versions, which mitigate the vulnerability.

- Post upgrading, terminate all active and persistent sessions (per appliance).

  – Connect to the NetScaler appliance using the CLI.

    - To terminate all active sessions, run the following command:

    ```
    kill aaa session -all
    ```

    - To clear persistent sessions across NetScaler load balancers, run the following command (where <vServer> is the name of the virtual server / appliance):

    ```
    clear lb persistentSessions <vServer>
    ```

    - To clear existing ICA sessions, run the following command:

    ```
    kill icaconnection -all
    ```

- Credential Rotation

  – Due to the lack of available log records or other artifacts of exploitation activity, as a precaution, organizations should consider rotating credentials for identities that were provisioned for accessing resources via a vulnerable NetScaler ADC or Gateway appliance.

  – If there is evidence of suspicious activity or lateral movement within an environment, organizations should prioritize credential rotation for a larger scope of identities if single factor authentication (SFA) remote access is allowed for any resources from the Internet.

- If web shells or backdoors are identified on NetScaler appliances, Mandiant recommends rebuilding the appliances using a clean-source image, including the latest firmware.

  Note: If a restoration of an appliance is required using a backup image, the backup configuration should be reviewed to ensure that there is no evidence of backdoors.

- If possible, reduce the external attack exposure and attack surface of NetScaler appliances by restricting ingress access to only trusted or predefined source IP address ranges.

Investigation

- To date, Mandiant has not identified any available logs or other artifacts resident on NetScaler appliances that record evidence of exploitation. Scoping an investigation has consisted of:
  - Reviewing NetScaler appliances for evidence of backdoors or web shells.
  - Identifying suspicious logons / lateral movement originating from published systems or resources accessible through the NetScaler appliances.
  - Correlating authentication and logon events (e.g., VDI systems published through NetScaler appliances) sourced from geographic locations that are not part of an established baseline.
  - Correlating authentication and logon events where a successful MFA challenge / response was not logged.

Detection

- If web application firewalls or other platforms that capture URL requests are deployed in front of NetScaler device(s), review available logs for an abnormal amount of web requests originating from suspicious IP addresses.

- If web application firewalls or other platform that capture URL requests are deployed in front of the NetScaler device(s), review for abnormal requests to the following URL path:

```
oauth/idp/.well-known/openid-configuration
```

  Note: This is a valid NetScaler URL path for retrieving information about configured OAuth IDP endpoints. Detection of suspicious requests will need to be baselined against historical expected connections to the URL path.

Linked Resources

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

https://docs.netscaler.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-persistence/clearing-persistence.html

https://developer-docs.netscaler.com/en-us/adc-command-reference-int/current-release/vpn/vpn-icaConnection.html#example

https://support.citrix.com/article/CTX234873/how-to-deploy-netscaler-as-both-oauth-sp-and-idp

https://github.com/mandiant/citrix-ioc-scanner-cve-2023-3519

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT®
NOW PART OF Google Cloud