Security Advisory 2023-075

Citrix NetScaler Critical Vulnerability

October 10, 2023 — v1.4

TLP:CLEAR

History:

- *10/10/2023 — v1.0 – Initial publication*
- *10/10/2023 — v1.1 – Fixed affected products list*
- *19/10/2023 — v1.2 – Added remediation and investigation informations from Mandiant*
- *26/10/2023 — v1.3 – Added additional remediation commands and detection informations*
- *03/11/2023 — v1.4 – Added additional detection informations*

Summary

On October 10, 2023, Citrix issued an advisory about multiple buffer-related vulnerabilities, **CVE-2023-4966** and **CVE-2023-4967**, affecting NetScaler ADC and NetScaler Gateway. These vulnerabilities can result in sensitive information disclosure and denial of service attacks [1].

It is recommended updating and remediating affected devices **as soon as possible**.

On October 19, 2023, Mandiant issued a remediation report regarding the vulnerability **CVE-2023-4966** [2]. Mandiant identified a zero-day exploitation of this vulnerability in the wild beginning in late August 2023.

On October 25, 2023, AssetIO brought more details [3] about the exploitation of **CVE-2023-4966** giving opportunities to detect a possible exploitation of the vulnerability. However, this requires an HTTP frontend source (e.g., network probe, WAF or reverse proxy) before reaching the Citrix HTTP services. A proof-of-concept is also available for that vulnerability [4].

[UPDATE] On November 2, 2023, Mandiant shared [5] information about artefacts that can be used to identify exploitation activity. Mandiant also shared their post exploitation techniques observation.

Technical Details

The vulnerability `CVE-2023-4966`, with as CVSS score of 9.4 out of 10, can lead to sensitive information disclosure. The appliance must be configured either as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or an AAA virtual server for exploitation.

Successful exploitation could result in the ability to hijack existing authenticated sessions, therefore bypassing multifactor authentication (MFA) or other strong authentication requirements. The sessions may persist after the update to mitigate CVE-2023-4966 has been deployed. Additionally, prior to the update being deployed, Mandiant observed session hijacking where session data was stolen and subsequently used by a threat actor [2].

The vulnerability `CVE-2023-4967`, with a CVSS score of 8.2 out of 10, can lead to a denial of service attack. The prerequisites for exploitation are the same as the above CVE.

Remediation

The Mandiant report [2] about the **CVE-2023-4966** contains the following remediation steps:

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

     Note: If the vulnerable appliances cannot be prioritised 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.
2. Upgrade Appliances
   - Upgrade vulnerable NetScaler ADC and Gateway appliances to the latest firmware versions, which mitigate the vulnerability.
3. Terminate Sessions
   - Post upgrading, terminate all active and persistent sessions (per appliance).
4. CLI Connection and Command
   - Connect to the NetScaler appliance using the CLI.
   - Run the following command (where `<vServer>` is the name of the virtual server / appliance).

```
kill icaconnection -all

kill rdp connection -all

kill pcoipConnection -all

kill aaa session -all

clear lb persistentSessions
```

5. Credential Rotation
   - Due to the lack of available log records or other artefacts of exploitation activity, as a precaution, organisations 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, organisations should prioritise credential rotation for a larger scope of identities if single factor authentication (SFA) remote access is allowed for any resources from the Internet.
6. Search for Web Shells or Backdoors
   - 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.

7. Restrict Ingress Access
    - 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

Mandiant has not identified any available logs or other artefacts 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 logon events / 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.

On October 25, 2023, AssetIO brought more details [3] about the exploitation of **CVE-2023-4966** giving opportunities to detect a possible exploitation of the vulnerability. However, this requires an HTTP frontend source (.e.g network probe, WAF or reverse proxy) before reaching the Citrix HTTP services.

Check the HTTP logs reaching the URI `/oauth/idp/.well-known/openid-configuration` with a GET method with the status code 200. If hits are found, check if the HTTP response bytes are above `1000000` or if the strings `aaaaaaaaaa` are in the HTTP host header.

[UPDATE] Mandiant has used the following approaches [5] to identify potential exploitation of **CVE-2023-4966** and subsequent session hijacking. These include the following techniques [5]:

- Investigating requests to the vulnerable HTTP/S endpoint from WAF: Analysing the incoming requests in the web application firewall logs to identify any unusual or malicious requests targeting the vulnerability, see above.
- Identifying suspicious login patterns based on NetScaler record syslog information in `/var/log/ns.log`:
    - Suspicious SSLVPN sessions can be identified by comparing the IP addresses recorded in the `Client_ip` and the `Source` fields in `TCPCONNSTAT` events. `TCPCONNSTAT` events record TCP connection-related information for a connection belonging to an SSLVPN session.
    - Identify source IP addresses that access multiple user accounts in a short period of time recorded in the `ns.log` files or forwarded logs via syslog. While a threat actor can choose only to access a single account from a single source IP address, Mandiant has observed that multiple accounts were accessed within hours from the same source IP address by a threat actor.
- Identifying evidence of exploitation using memory analysis of NetScaler Memory Core Dump Files: In some cases, evidence of exploitation can be found in the memory space

of the `NSPPE` process of the appliance. Exploitation of CVE-2023-4966 will not crash the `NSPPE` process and generate memory core dump files. To perform analysis of NetScaler memory core dump files, they need to be collected. It is important not to reboot the appliance prior to generating a core dump for analysis.

[UPDATE] Following the successful exploitation of **CVE-2023-4966**, Mandiant observed the following TTPs:

- Host and network reconnaissance.
- Credential harvesting.
- Lateral movement via RDP.
- Active Directory reconnaissance using living-off-the-land binaries (e.g., `net.exe`).
- Internal network enumeration using SoftPerfect network scanner (`netscan.exe`).
- Compressing reconnaissance results using 7-zip and encoding segments with `certutil`.
- Loading malicious DLLs into lsass process memory to create a memory dump for offline credential extraction.
- Deployment of a newly tracked backdoor, `FREEFIRE`, which uses Slack for command and control.
- Deployment of remote monitoring and management (RMM) tools like Atera, AnyDesk, and SplashTop to maintain a foothold post-exploitation.

Affected Products

- 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 vulnerable [1].

Recommendations

CERT-EU recommends updating and remediating affected devices as soon as possible. CERT-EU also recommends investigating all affected devices.

References

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

[2] https://services.google.com/fh/files/misc/citrix-netscaler-adc-gateway-cve-2023-4966-remediation.pdf

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

[4] https://github.com/assetnote/exploits/blob/main/citrix/CVE-2023-4966/exploit.py

[5] https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966