FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

31 JAN 2020

AC-000116-TT

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the **Reporting Notice** section of this message.

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Unidentified Cyber Actors Exploit Citrix Vulnerability to Gain Access to Networks

Summary

Beginning mid-January 2020, unidentified cyber actors have used a Citrix vulnerability, **CVE-2019-19781**, in an attempt to exploit hundreds of U.S. networks, to include private companies, educational institutions, healthcare-related infrastructure, and local and federal government domains. The actors have used a a variety of Python, Perl, and shell scripts to exploit vulnerable Citrix servers and have exfiltrated the Netscaler configuration key store. A variety of Tactics, Techniques, and Procedures (TTPs) have been observed, likely indicating multiple criminal and nation-state actors are exploiting this vulnerability to accomplish a variety of objectives. It is also possible that adversaries already exploited this vulnerability prior to patch development/deployment.

Threat: Citrix Server Vulnerability (CVE-2019-19781)

On December 17, 2019, Citrix released a security bulletin (CTX267027) describing a vulnerability in Citrix Application Delivery Controller (ADC), Citrix Gateway, and two older versions of Citrix SD-WAN WANOP. The vulnerability allows an attacker to gain unauthorized access to published applications and other internal network resources from the Citrix servers,

and eventually leads to a remote code execution. Although a fix for the issue was not yet available to owners of Citrix servers when the security bulletin was first released, Citrix published steps owners may take to mitigate the possibility of an attack leveraging that vulnerability. The vulnerability, assigned CVE-2019-19781, has been deemed Critical in severity as it could allow an unauthenticated attacker to perform arbitrary remote code execution on vulnerable gateways.

As of January 10, 2020, proof-of-concept code allowing for exploitation of CVE-2019-19781 was publicly available, prompting widespread scanning for vulnerable Citrix applications. On January 19, 2020, Citrix began releasing patches, with full patches released on January 24, 2020.

The vulnerability enables a directory traversal attack on the /vpn directory of the Netscaler that will allow arbitrary file access and code execution as the user "nobody." This access can also enable access to sensitive data such as Netscaler config key store. This stores all the used login credentials for the Virtual Machine's on the other side of the gateway, which may include Windows domain credentials. If the device is not configured properly, this store will be encrypted using a widely known default key.

Successful exploitation will often result in xml files being written to folders within the /var subdirectory. The file names will usually be random and likely indicate successful remote code execution. FBI analysis on these file names indicated some of them matched file names related to open source exploit kits available online.

A variety of different actor groups have been observed exploiting this vulnerability to deliver a variety of payloads, which to date have included netcat listeners and SOCKS proxies to enable internal network access, backdoors to enable remote access, and even a Monero cryptocurrency miner.

Widespread scanning for the Citrix ADC and Gateway vulnerability (CVE-2019-19781) has been reported. The scanning included HTTP GETs for *"/vpn/../vpns/cfg/smb.conf"* and HTTP POSTs for *"/vpn/../vpns/portal/scripts/newbm.pl*".

The actors have been observed using the newbm.pl Perl Script to write a Python version of the Netcat network utility application (rtcp.py) onto the

target's Citrix server at the location "*netscaler/portal/scripts/rtcp.py*." From there, the actors would be able to send connections from the Citrix server to the actors' C2. Actors have also been known to upload and use the reGeorg network tunneling tool.

Because this exploit allows an attacker to remotely execute any arbitrary code capable of running on the Netscaler platform's FreeBSD operating system, attackers may deploy new tools or techniques at any time.

The FBI has found that the following IOCs have been used in attacks against multiple U.S. entities.

IP Addresses:			
188.166.106.153	192.3.255.144	31.134.200.75	51.68.122.93
81.110.55.125	82.27.64.190	109.70.100.22	37.220.31.72
185.118.166.67	193.187.174.104	185.178.45.221	95.179.163.186
61.218.225.74	104.168.148.236	142.11.236.143	192.236.192.4
23.254.164.48	185.118.166.116	192.236.192.3	104.168.166.234
23.254.164.181	142.11.211.250	185.144.30.151	62.113.112.33
209.58.167.82	213.168.251.57	217.12.221.12	5.101.0.209
23.129.64.153	23.239.25.190	34.92.135.167	45.32.45.46
45.33.92.155	45.79.129.215	45.79.16.27	45.79.29.24
47.52.196.152	50.116.54.30	69.164.202.142	77.247.181.162
83.97.20.221	85.90.247.110	104.248.173.74	128.199.142.71
138.68.108.109	138.68.63.197	139.162.169.180	139.162.189.189
139.59.212.187	139.59.215.190	142.93.150.162	142.93.158.201
157.245.226.196	162.243.1.231	167.172.39.20	167.172.39.22
167.71.152.130	167.99.111.51	172.104.210.59	172.104.214.114
172.105.64.188	172.105.90.222	173.255.200.120	176.10.99.200
176.58.104.222	176.58.109.238	185.234.216.20	188.166.9.236
192.241.254.112	192.241.255.149	193.56.28.185	193.57.40.46
206.189.208.169			

Tools and Files:	
Filename or Tool	*Comment*
URL (HTTP GET)	http://[Victim IP address or domain]/vpn/../vpns/cfg/smb.conf

URL (HTTP POST)	http://[Victim IP address or domain]/vpn/../vpns/portal/scripts/<any script file>
URL (HTTP GET)	http://[Victim IP address or domain]/vpn/../vpns/portal/*.xml
/netscaler/portal/templates	Likely backdoor location
/var/tmp/netscaler/portal/templates	Likely backdoor location
/var/vpn/bookmark/*.xml	Bookmark indicating compromise
/var/vpn/bookmark/user1337.xml	Bookmark indicating compromise
/var/vpn/bookmark/pwnpzil1337.xml	Bookmark indicating compromise
tunnel.[ashx|aspx|js|jsp|php]	reGeorg webshell
/vpn/../vpns/portal/scripts/newbm.pl	Malicious PERL script
/vpn/../vpns/portal/scripts/ci.sh	Backdoor shell script Md5: 0e431d0d9e0fc371c163e4de5226c50b
/netscaler/portal/scripts/rtcp.py	Python version of Netcat
/var/tmp/nspps	Go backdoor Md5: 568f7b1d6c2239e208ba97886acc0b1e Alternate version: Md5: 1c8c28e4db5ad7773da363146b10a340
/var/tmp/netscalerd	Monero miner Md5: 5be9abbe208a1e03ef3def7f9fa816d3

Snort rule for the detecting Perl Script on victim networks:

capture_packets tcp any any <> any any (msg: “# Malicious Perl script traffic # post Citrix exploit"; content: "POST"; offset: 0; depth: 4; content: "User-Agent: Mozilla/5.0 (Macintosh\|3b\| Intel Mac OS X 10.14\|3b\| rv:71.0) Gecko/20100101 Firefox/71.0"; distance: 0; within: 300; content: "desc: desc"; distance: 0; within: 100;)”

Snort rule for detecting unmodified version of reGeorg activity on a network:

capture_packets tcp any any <> any any (msg: "REGEORG Tunnel # X_STATUS Response"; content: "X-STATUS:"; fast_pattern; offset: 20; depth: 500; content: "HTTP/1.1 200 OK"; offset: 0; depth:15; pcre: "/X-STATUS: (OK\|FAIL)\x0d\x0a/";)

capture_packets tcp any any <> any any (msg: "REGEORG Tunnel # X_CMD POST"; content: "XCMD:"; fast_pattern; offset: 20; depth: 500; content: "POST"; offset: 0; depth: 4; pcre: "/?cmd=(read|connect|disconnect|forward)/i";)

A free tool to scan for IOC's related to this vulnerability has been released on GitHub:
https://github.com/fireeye/ioc-scanner-CVE-2019-19781/releases/tag/v1.0

https://github.com/cisagov/check-cve-2019-19781

A link of the following form can be used to determine if a system is affected:
https:// CITRIXGATEWAY /vpn/../vpns/cfg/smb.conf

For example, the following curl command can be used:
curl https:// CITRIXGATEWAY /vpn/../vpns/cfg/smb.conf --path-asis -k –f

The " CITRIXGATEWAY " string should be replaced with the name or IP of the system you wish to test. If retrieving the link results in a 403 Forbidden error, then the mitigations outlined below have likely been applied. However, if retrieving the link results in the contents of a smb.conf file, then the system is vulnerable.

Recommendations

The FBI recommends the following steps to help reduce the overall risk from these exploitation attempts.

- Be alert to and immediately install patches released by vendors, especially for web-facing appliances;
- Check Citrix Netscaler appliances for any suspicious scripts or running processes;
- Block or monitor the above malicious IP addresses, as well as any other IP addresses conducting remote logins outside of regular business hours;
- Implement network segmentation where appropriate;

- Ensure that Netscaler appliances are using the latest encryption version for their config key stores;
- Check for vulnerable appliances by performing a GET request to: https://{host}/vpn/../vpns/. If the response is not "You don't have permission to access /vpns/", the system is likely vulnerable.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). With regards to specific information that appears this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's national Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN** information may not be released outside of the community.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.