National Cyber Security Centre

a part of GCHQ

Alert: Actors exploiting a vulnerability in Citrix ADC and Gateway products

14 January 2020

© Crown Copyright 2020

Details

The NCSC is investigating exploitations of a critical vulnerability in the Citrix Application Delivery Controller (ADC) and Citrix Gateway that could allow an unauthenticated attacker to perform arbitrary code execution on a network. The vulnerability is CVE-2019-19781 and its exploitation has been widely reported online in early January.[1]

The following Citrix products are affected:

- 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

Mitigation

Citrix initially disclosed this vulnerability in an Advisory on 17 December 2019.[2] There is currently no patch, although Citrix have advised customers that updates for affected products will be available from 20 January 2020 onwards, depending on the product.

Before a patch is released, Citrix have provided mitigation advice **which the NCSC strongly advises organisations to implement**. Full details of how to mitigate are on the Citrix website.[3] Organisations are advised to check the Citrix website to keep up to date with patch releases.

The NCSC also recommends that organisations carry out searches across their networks to identify whether exploitation has taken place, if they did not implement these mitigations before Citrix disclosed the vulnerability on 17 December 2019.

Detection

The following can be used as a simple check for a vulnerable system:

1. Perform a GET request to: https://{host}/vpn/../vpns/
2. Check response for "You don't have permission to access /vpns/"

An Australian Cyber Security Centre Advisory provides useful detection advice for network defenders.[4] To detect a compromise on SSL VPN configurations, review Citrix web request logs for:

[1] For more background see: https://www.tripwire.com/state-of-security/vert/citrix-netscaler-cve-2019-19781-what-you-need-to-know/ and https://www.reddit.com/r/blueteamsec/comments/en4m7j/multiple_exploits_for_cve201919781_citrix/
[2] https://support.citrix.com/article/CTX267027
[3] https://support.citrix.com/article/CTX267679
[4] https://www.cyber.gov.au/threats/advisory-2020-001-active-exploitation-critical-vulnerability-citrix-application-delivery-controller-and-citrix-gateway

- HTTP log messages starting with “/vpn/../” containing directory traversal attacks such as “/vpn/../vpns/portal/scripts/newbm.pl” or “/vpn/../vpns/cfg/smb.conf” or “/vpn/../vpns/portal/scripts/newbm.pl”
- A direct request logged to “/vpns/” without the xml specified
- A POST followed by a GET to an XML file

In addition, there are some attack paths that do not require path traversal. For example:

```
POST /vpns/portal/scripts/newbm.pl HTTP/1.1
Host: <target>
NSC_USER: ../../../netscaler/portal/templates/si
NSC_NONCE: 5
Content-Length: 53
url=a&title=[%+http://template.new({'BLOCK'='print+id'})%]
```

The HTTP response code 304 indicates the Citrix server has previously been exploited. As versions of these logs may be compressed due to file size limits or aging, network defenders should ensure archived versions are also checked.

If malicious activity is noted in the above logs, further analysis is recommended:

- Process Listing: Triage all child processes of “httpd” and look for any suspicious processes owned by user ‘`nobody`’
- File System: Look for any recently created or unusual XML files, specifically in locations which can be written to or allow execute permissions such as: /netscaler/portal/templates or /var/tmp/netscaler/portal/templates
- bash.log: This file contains information on command executions even if the environment variable HISTFILE has been unset. Look for any suspicious executables such as curl, hostname, uname, or whoami, or commands run by user ‘`nobody`’.

Organisations who detect any suspected exploitation should report to the NCSC via the website at https://report.ncsc.gov.uk/.

Additional information

A Sigma rule to detect activity is publicly available:[5]

```
title: Citrix Netscaler Attack CVE-2019-19781
description: Detects CVE-2019-19781 exploitation attempt against
Citrix Netscaler, Application Delivery Controller and Citrix Gateway
Attack
id: ac5a6409-8c89-44c2-8d64-668c29a2d756
references:
    - https://support.citrix.com/article/CTX267679
    - https://support.citrix.com/article/CTX267027
    - https://isc.sans.edu/diary/25686
    - https://twitter.com/mpgn_x64/status/1216787131210829826
author: Arnim Rupp, Florian Roth
status: experimental
date: 2020/01/02
modified: 2020/01/13
logsource:
    category: webserver
    description: 'Make sure that your Netscaler appliance logs all
kinds of attacks (test with http://your-citrix-gw.net/robots.txt)'
detection:
    selection:
        c-uri-path:
            - '*/../vpns/*'
            - '*/vpns/cfg/smb.conf'
            - '*/vpns/portal/scripts/newbm.pl*'
            - '*/vpns/portal/scripts/rmbm.pl*'
            - '*/vpns/portal/scripts/picktheme.pl*'
    condition: selection
fields:
    - client_ip
    - vhost
    - url
    - response
falsepositives:
    - Unknown
level: critical
```

[5] https://github.com/Neo23x0/sigma/blob/master/rules/web/web_citrix_cve_2019_19781_exploit.yml

In addition, the following Snort rule alerts on the first part of the "Project Zero India" exploit:[6]

```
alert tcp any any -> any any (sid: 1019781; msg: "SERVER-WEBAPP
Citrix ADC NSC_USER directory traversal attempt"; content:
"NSC_USER:"; fast_pattern; content: "NSC_USER:"; http_header;
content: "/../"; http_header; content: "POST"; http_method; content:
"NSC_NONCE:" ; http_header; content: ".pl"; http_uri; content:
"/vpns/"; http_uri; reference:cve,2019-19781; classtype: web-
application-attack)
```

Exploitation code is also available at the links below:

https://github.com/projectzeroindia/CVE-2019-19781

https://github.com/ianxtianxt/CVE-2019-19781

https://github.com/trustedsec/cve-2019-19781/blob/master/citrixmash.py

https://github.com/jas502n/CVE-2019-19781/blob/master/CVE-2019-19781.py

https://github.com/rapid7/metasploit-framework/pull/12816/commits/50637d0d917a78f5eba5281f634df0af314d8d55

https://github.com/Jabo-SCO/Shitrix-CVE-2019-19781/blob/master/README.md

[6] https://isc.sans.edu/forums/diary/Citrix+ADC+Exploits+are+Public+and+Heavily+Used+Attempts+to+Install+Backdoor/25700/