A Quick Update on Scanning for CVE-2019-19781 (Citrix ADC / Gateway Vulnerability)

Published: 2020-01-07. **Last Updated**: 2020-01-07 13:16:10 UTC
by Johannes Ullrich (Version: 1)

2 comment(s)

For the last week, I have been monitoring our honeypot logs for evidence of exploits taking advantage of CVE-2019-19781. Currently, I have not seen an actual "exploit" being used. But there is some evidence that people are scanning for vulnerable systems. Based on some of the errors made with these scans, I would not consider them "sophisticated." There is luckily still no public exploit I am aware of. But other sources I consider credible have indicated that they were able to create a code execution exploit.

The most basic scan I have seen is a simple "GET" request for "/vpns/." For example:

```
GET /vpns/ HTTP/1.1
Host: [redacted ip address of host]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0)
Gecko/20100101 Firefox/71.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

For a Citrix ADC appliance, this request will return a 403 Forbidden status, even if the workaround was not applied. For most other web applications, it will return a 404 error. This request can be used to identify a Citrix ADC server, but it does not show if the server is vulnerable.

A more exciting request:

```
GET /vpns/cfg/smb.conf HTTP/1.1
Host: [ redacted IP address of honeypot ]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.
```

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

```
NSC_USER: admin4123
NSC_NONCE: 123456
NSC_CLIENTTYPE: 123
Connection: close
Upgrade-Insecure-Requests: 1
```

Interestingly, this client first hit the index page and downloaded all related assets, including favicon. The initial requests used a different user agent, and it kind of looks like the individual did first some manual pre-qualification of the honeypot before hitting this URL. But the real shocker (or not... if you looked at the code for a while) is that yes, smb.conf is exposed and can be retrieved without authentication. I tested it on an "unconfigured" virtual appliance (meaning I just downloaded it and didn't set up any features on it). The "NCS" headers are also typical for "Netscaler" but not required for this particular request. smb.conf is the only file in this directory.

Other requests show fewer skills (or I just don't understand what they are trying to accomplish):

GET //vpns/script/vista/*.exe HTTP/1.1" 404 493 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"

Yes, there is an executable in this directory. But the wildcard URL doesn't work. Does it ever? This may be someone who red the advisory but didn't quite understand that part.

Another more dangerous request:

```
POST //vpns/portal/scripts/newbm.pl?url=[source IP
redacted]&title=1232&desc=12312&UI_inuse=RfWeb HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:71.0)
Gecko/20100101 Firefox/71.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0, no-cache
Origin: http://[honeypot ip redacted]
Pragma: no-cache
Content-Length: 0
```

This request doesn't trigger an exploit the way it is written, and wouldn't work "as is" (parts missing). But it does hit one of the vulnerable URLs. So far, I only saw two requests, and they appeared to come from the same source (different source IPs, but close to each other in time and similar requests overall).

Source IPs scanning the honeypot for any of these URLs so far:

117.186.7.127 China Mobile
213.252.247.236 BACloud (Europe/US colo servers)
223.167.22.29 CHINA UNICOM Shanghai city network
94.247.167.104 OpenIP (France DSL)

A quick note on signatures I have seen: At least partial exploitation (file upload, data leakage) is possible without a "/../" pattern in the URL. Signatures should only look for the "/vpns/" pattern in the URL.

Johannes B. Ullrich, Ph.D., Dean of Research, SANS Technology Institute
Twitter|

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

Keywords: citrix CVE201919781 netscaler

2 comment(s)

previous next

Comments

I've published some additional guidance about this here: https://www.tripwire.com/state-of-security/vert/citrix-netscaler-adc-cve-2019-19781/

Please note that the exploitation process is different depending on whether the ADC IP or the VIP is exposed.

Anonymous
Jan 8th 2020
4 years ago

Will the Netscaler/ADC GeoIP feature reduce the attack surface?
https://support.citrix.com/article/CTX130701

Anonymous
Jan 10th 2020
4 years ago

Login here to join the discussion.

Top of page

Diary Archives