SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Directory Traversal Schwachstelle in Citrix Application Delivery Controller und Gateway (CVE-2019-19781)

Erfolgreiche Ausnutzung erlaubt Remote-Code-Ausführung (RCE)

CSW-Nr. 2020-172597-1731, Version 1.7, 17.09.2020

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Der US-Software-Hersteller Citrix bietet u. a. mit den beiden Produkten Citrix Gateway (ehemals NetScaler Gateway) und Citrix Application Delivery Controller (ADC, ehemals NetScaler ADC) ein VPN-Gateway für den entfernten Zugriff auf organisationsinterne Anwendungen an. Citrix ADC weist dabei im Vergleich zu dem Citrix Gateway mehr Funktionen wie Load Balancing, Web Application Firewall etc. auf. Der Login erfolgt bei beiden Produkten über einen Web-Browser, der Einsatz einer Zwei-Faktor-Authentifizierung (2FA) dient häufig der Absicherung von Benutzername und Passwort.

Das Citrix Gateway und der Citrix ADC weisen jeweils eine Directory Traversal Schwachstelle [Mitre] auf, die mithilfe von präparierten URL-Anfragen durch einen nicht authentifizierten Angreifer ausgenutzt werden kann, um Konfigurationen auszulesen, Dateien abzulegen oder Code auszuführen. Die Schwachstelle CVE-2019-19781 kann den Zugriff auf normalerweise nicht öffentlich zugreifbare Verzeichnisse erlauben.

Citrix hat am Samstag, 11.01.2020 den Veröffentlichungszeitplan für Sicherheitsupdates zur Behebung der Directory Traversal Schwachstelle CVE-2019-19781 genannt [Citrix01]:

Citrix ADC und Citrix Gateway

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Firmware-Versionszweig	Aktualisierte Build-Version	~~Geplantes~~ Veröffentlichungsdatum
10.5	10.5.70.12	~~Freitag, 31. Januar 2020~~ Freitag, 24. Januar 2020
11.1	11.1.63.15	~~Montag, 20. Januar 2020~~ Sonntag, 19 Januar 2020
12.0	12.0.63.13	~~Montag, 20. Januar 2020~~ Sonntag, 19 Januar 2020
12.1	12.1.55.18	~~Montag, 27. Januar 2020~~ ~~Freitag, 24. Januar 2020~~ Donnerstag, 23. Januar 2020
13.0	13.0.47.24	~~Montag, 27. Januar 2020~~ ~~Freitag, 24. Januar 2020~~ Donnerstag, 23. Januar 2020

Update 1:
Am Donnerstag, 16.01.2020 wurde die Citrix SD-WAN WANOP Appliance als betroffenes Produkt ergänzt [Citrix01].

Citrix SD-WAN WANOP

Firmware-Versionszweig	Aktualisierte Build-Version	Geplantes Veröffentlichungsdatum
10.2.6b	11.1.51.615	~~Montag, 27. Januar 2020~~ ~~Freitag, 24. Januar 2020~~ Mittwoch, 22. Januar 2020
11.0.3b	11.1.51.615	~~Montag, 27. Januar 2020~~ ~~Freitag, 24. Januar 2020~~ Mittwoch, 22. Januar 2020

Die Sicherheitsupdates werden über die Citrix-Webseiten für Citrix ADC [Citrix02] und Citrix Gateway [Citrix03] bereitgestellt.

Bis zur Veröffentlichung der Sicherheitsupdates stellt Citrix eine Konfiguration zur Filterung von Directory Traversal Anfragen als Workaround zur Verfügung [Citrix04].

Update 1:
Am 16.01.2020 hat Citrix des Weiteren in dem Security Bulletin auf ein Skript zur Prüfung [Citrix06] der erfolgreichen Umsetzung des Workarounds verwiesen.

Seit Dienstag, 07. Januar 2020 informiert das BSI über CERT-Bund Reports [BSI01] deutsche Netzbetreiber zu öffentlich erreichbaren Citrix-Systemen, die den Workaround noch nicht umgesetzt haben [Twitter01].

Es sind im Internet erhöhte Scans nach verwundbaren Citrix ADC und Gateway Installationen zu verzeichnen. Entsprechende Scan- und Exploit-Skripte sind inzwischen öffentlich verfügbar [Reddit].

Update 1:
Das BSI beobachtet auf Basis von Rückmeldungen betroffener Organisationen eine aktive Ausnutzung der Citrix-Schwachstelle CVE-2019-19781. Aus diesem Anlass wurde am 16.01.2020 eine BSI Pressemitteilung veröffentlicht [BSI06].

Update 2:
Seit dem 19.01.2020 liefert Citrix einen Patch für die Versionen 12.0 und 11.1 des Citrix ADC und Citrix Gateway [Citrix01].

Für die restlichen betroffenen Produkte und Versionen hat Citrix die Veröffentlichung auf den 24.01.2020 vorgezogen [Citrix01].

Update 3:
Am 22.01.2020 hat Citrix gemeinsam mit FireEye / Mandiant einen Indicator of Compromise Scanner veröffentlicht [Citrix07], der von der Citrix-Schwachstelle CVE-2019-19781 betroffene Systeme auf Spuren einer Kompromittierung untersucht. Auf dem Citrix-System werden dabei bekannte Angriffspunkte geprüft. Die Ergebnisse des Scanners sind in drei Kategorien eingeteilt:

1. Evidence of compromise / Hinweise auf eine erfolgreiche Kompromittierung
2. Evidence of successful vulnerability scanning / Hinweise auf erfolgreiche Schwachstellen-Scans und damit verwundbaren Zustand
3. Evidence of failed vulnerability scanning / Hinweise auf fehlgeschlagene Schwachstellen-Scans

Als Unterstützung bei der Risikobewertung der Citrix-Schwachstelle CVE-2019-19781 stellt NCSC.NL ein Flussdiagramm zur Verfügung [NCSC.NL01].

Update 4:
Am 24.01.2020 hat Citrix die letzten Sicherheitsupdates für den Versionszweig 10.5 der betroffenen Citrix ADC und Citrix Gateway Systeme veröffentlicht. Bereits am 23.01.2020 sind die Sicherheitsupdates für die Versionszweige 12.1 und 13.0 veröffentlicht worden [Citrix01].

Update 6:
Dem BSI liegen Hinweise vor, dass die Ausnutzung der Schwachstelle CVE-2019-19781 im Citrix ADC und Gateway aktuell erneut im Kontext von Ransomware-Angriffen zu beobachten ist. Frühe Angriffe wurden im Januar und Februar 2020 öffentlich bekannt [Fireeye02] [BLC2020]. Betroffen können auch im Januar 2020 gepatchte Citrix-Systeme sein, welche allerdings vor der Installation der Citrix-Sicherheitsupdates kompromittiert wurden und somit Angreifenden potenziell den Zugriff auf interne Netze erlauben. Es gelten weiterhin die unten empfohlenen Maßnahmen. Handlungsempfehlungen zu Ransomware Prävention und Reaktion stellt das BSI öffentlich zur Verfügung [BSI07].

Update 7:
Dem BSI werden zunehmend Vorfälle bekannt, bei denen Citrix-Systeme bereits vor der Implementierung des Workarounds bzw. der Installation der Sicherheitsupdates kompromittiert wurden. Dabei wurden Hintertüren (Backdoors) eingeschleust, welche Angreifern auch nach Schließung der Sicherheitslücke weiterhin Zugriff auf das Citrix-System und dahinterliegende Netzwerke ermöglichten. Diese Hintertüren werden jetzt vermehrt ausgenutzt, um Angriffe auf betroffene Organisationen durchzuführen. Hierzu wird auch von externen IT-Sicherheitsdienstleistern berichtet [HiSolutions].

Bewertung

Aufgrund der zu beobachtenden Schwachstellen-Scans und veröffentlichter Exploit-Skripte stellt die Schwachstelle je nach lokaler Netzkonfiguration ein mögliches Einfallstor in interne Netze dar. Es ist davon auszugehen, dass die Exploit-Skripte großflächig genutzt werden. Daher sollte der von Citrix genannte Workaround umgehend angewendet werden. Ebenso sollte mit den für Ende Januar 2020 angekündigten Sicherheitsupdates verfahren werden.

Update 1:
Bei der aktiven Ausnutzung der Schwachstelle werden diverse Payloads beobachtet, die von dem Auslesen von Konfigurationsdateien über Skripte zur Generierung von Krypto-Währungen bis hin zu der Einrichtung von sogenannten Reverse Shells für den entfernten Zugriff auf Kommandozeile reichen [Fireeye01], [SANS], [TrustedSec01]. Auf verwundbaren Citrix-Systemen, bei denen der Workaround nicht oder erst vor kurzem umgesetzt wurde, ist eine bereits erfolgte Kompromittierung wahrscheinlich. Daher sollten die in den Maßnahmen empfohlenen Suchansätze nach möglichen Kompromittierungen durchgeführt werden.

Update 3:
Der von Citrix und FireEye / Mandiant am 22.01.2020 veröffentlichte Indicator of Compromise Scanner [Citrix07] prüft die bekannten Angriffspunkte bei der Ausnutzung der Citrix-Schwachstelle CVE-2019-19781 und kann damit eine Kompromittierung nicht mit vollständiger Sicherheit ausschließen. Daher sollte zusätzlich ein eigenes Monitoring der Citrix-Infrastruktur erfolgen.

Des Weiteren liegen dem BSI inzwischen aus mehreren Quellen Hinweise vor, dass eine erfolgreiche Ausnutzung der Citrix-Schwachstelle CVE-2019-19781 bereits am 08.01.2020 beobachtet wurde. Daher müssen alle Citrix-Systeme, die den Workaround [Citrix04] zur Filterung maliziöser Anfragen nicht vor dem 08.01.2020 umgesetzt hatten, als potenziell kompromittiert betrachtet werden.

Update 6:
Die Ausnutzung der Citrix-Schwachstelle für Ransomware-Angriffe zeigt, dass selbst gepatchte Systeme, die allerdings zuvor kompromittiert wurden, für weitergehende Angriffe genutzt werden können. Umso wichtiger ist die unter den Maßnahmen genannte Überprüfung des Kompromittierungsstatus der Citrix ADC und Gateway Systeme sowie in dem Fall die Ableitung der unten aufgeführten Maßnahmen im Falle einer Kompromittierung.

Update 7:
Es ist davon auszugehen, dass eine große Anzahl von Citrix-Systemen bereits vor der Implementierung des Workarounds bzw. Installation der Sicherheitsupdates von Angreifern kompromittiert und Hintertüren eingeschleust wurden. In vielen Fällen wurde die Kompromittierung nicht erkannt, sodass Angreifer auch nach Schließung der Sicherheitslücke weiterhin Zugriff auf die Systeme und dahinterliegende Netzwerke hatten. Auf diesem Wege konnten Angreifer potenziell über mehrere Monate auf die Netzwerke betroffener Organisationen zugreifen und ggf. sensible Informationen ausspähen. Aktuell werden vermehrt Angriffe mit Ransomware auf betroffene Organisationen durchgeführt.

Erfolgreiche Angriffe unter Ausnutzung der Hintertür haben zur Folge, dass die betroffenen Organisationen ihren Betrieb extrem einschränken oder sogar einstellen müssen. Betriebsabläufe stehen still, Dienstleistungen können nicht mehr erbracht werden, mit zum Teil erheblichen Folgen für Kunden und Gesellschaft. Dies kann von Gewinnverlusten, Schadensersatzklagen, Vertrauensverlust bis hin zur Schädigung an Leib und Leben führen [BSI08].

Das BSI empfiehlt daher nachdrücklich, alle Citrix-Systeme auf eine potenzielle Kompromittierung hin zu überprüfen. Sofern sich Hinweise auf eine Kompromittierung ergeben, sollten die unten aufgeführten Maßnahmen unbedingt zeitnah umgesetzt werden. Insbesondere sollten betroffene Systeme komplett neu aufgesetzt, die Zugangsdaten aller Nutzer geändert und TLS-Zertifikate widerrufen und ausgetauscht werden.

Sollte Ihr IT-Betrieb nicht über die notwendigen Kompetenzen zur Untersuchung der Systeme auf Kompromittierungen verfügen, ziehen Sie einen externen IT-Sicherheitsdienstleister zurate.

Das Unterlassen entsprechender Absicherungsmaßnahmen kann eine grob fahrlässige Verletzung von - insbesondere auch gesetzlichen - Absicherungspflichten darstellen und im Falle von Datenabfluss, Datenverlust oder des Ausfalls Ihres Netzwerks auch zu Schadensersatzansprüchen oder Bußgeldern führen.

Im Rahmen der Bearbeitung von Vorfällen stellt das BSI immer wieder fest, dass die Kosten und Aufwände für die Umsetzung präventiver IT-Sicherheitsmaßnahmen sowie externe fachliche Beratung und Unterstützung deutlich niedriger ausfallen als die Kosten und Aufwände zur Reaktion auf einen erfolgreichen Angriff. Nach einem Angriff gilt es zum Beispiel, ein umfangreich kompromittiertes Netzwerk inklusive der Active-Directory-Infrastruktur kurzfristig und mit deutlichem Restrisiko zu härten und in einen Notbetrieb zu nehmen sowie parallel komplett neu aufzubauen. Bei Ransomware-Angriffen müssen verschlüsselte Daten aufwendig von Backups rekonstruiert oder gar nach Lösegeldzahlung (auf die Bereitstellung der Schlüssel durch die Täter angewiesen) entschlüsselt werden. Falls die Täter auch gestohlene Daten veröffentlichen, kommen ggf. hohe Kosten und Aufwände für die Kunden- und Partnerkommunikation, Datenschutz-Compliance oder den Verlust von Geschäftsinterna auf nicht ausreichend präventiv agierende Organisationen zu. Das jeweilige Management muss den Schutz der IT-Infrastruktur unter dieser Bedrohungslage angemessen unterstützen!

Maßnahmen

Bis zur Bereitstellung von Sicherheitsupdates zur Behebung der Directory Traversal Schwachstelle CVE-2019-19781 durch Citrix sollte der empfohlene Workaround [Citrix04] unmittelbar auf Citrix Gateway und Citrix ADC Systemen umgesetzt werden, um eine Ausnutzung zu verhindern. Bei Standard-Images von Cloud-Service-Providern ist es möglich, dass sie den Workaround noch nicht enthalten [Twitter02].

Update 1:
Bei dem Citrix ADC Release 12.1 ist eine Build-Version mindestens ab dem aktualisierten 12.1 Build 50.28/50.31 ~~51.16/51.19 und 50.31~~ zu nutzen, da der Workaround ansonsten nicht greift [Citrix01].

Update 2:
Für die für Citrix ADC und Citrix Gateway Versionen 12.0 und 11.1 sollten die am Sonntag, 19.01.2020 veröffentlichten Sicherheitsupdates zeitnah installiert werden. Ebenso ist mit den für Freitag, 24.01.2020 für die restlichen betroffenen Versionen angekündigten Sicherheitsupdates zu verfahren.

Update 3:
Sofern der Workaround auf verwundbaren Citrix-Systemen nicht vor dem 08.01.2020 umgesetzt wurde, sollten die Citrix-Systeme entweder manuell auf Basis der folgenden Hinweise oder mit dem Citrix / FireEye Scanner [Citrix07] geprüft werden. Die Nutzung des Scanners kann außerdem zusätzlich zu der manuellen Prüfung erfolgen.

Mögliche Angriffsversuche über präparierte Directory Traversal Anfragen sind in den Citrix-Logs zu finden [Twitter03], z. B.:

```
# gzcat /var/log/http* | grep "/../vpns/"
```

Weitere Suchansätze stellen die Bash-History, laufende Prozesse und kürzlich angelegte Dateien in den Template-Verzeichnissen dar [TrustedSec02], [Winkel] z. B.

Update 1:

Ort der Angreiferspuren	Befehl	Hinweis
Apache-Logs	cat /var/log/httpaccess.log | grep vpns | grep xml gzcat /var/log/httpaccess.log.*.gz | grep vpns | grep xml cat /var/log/httpaccess.log | grep "/\.\./" gzcat /var/log/ httpaccess.log.*.gz | grep "/\.\./"	Suche nach Scan- und Exploit-Aktivitäten in den Apache-Logs. Interessant sind zudem Zugriffe auf evtl. platzierte Webshells.
Bash-Logs	cat /var/log/bash.log | grep nobody gzcat /var/log/bash.*.gz | grep nobody	Da bei der Ausnutzung der Schwachstelle die Rechte des Webservers zum Einsatz kommen, ist es sinnvoll nach den Bash-Aktivitäten des Benutzers "nobody" zu suchen.
Laufende Prozesse	ps auxd | grep nobody ps -aux | grep python ps -aux | grep perl	Anzeige aller Prozesse, die mit dem Benutzer "nobody" laufen. Alles außer /bin/httpd ist verdächtig. Des Weiten Suche nach evtl. maliziösen Python-/Perl-Skripten.
Cronjobs	crontab -u <username> -l	Prüfung, ob für vorhandene Benutzer Cronjobs angelegt worden sind (vgl. [Winkel]).
Citrix-Bash/FreeBSD-Benutzer	cat /etc/passwd	Prüfung, ob neue Benutzer hinzugefügt worden sind (vgl. [Winkel]).
XML-Dateien initialer Exploits	ls -latr /netscaler/ portal/templates/*.xml ls -latr /var/tmp/ netscaler/portal/templates	Alle XML-Dateien in diesen Verzeichnissen, die nach dem 17.12.2019 (initiale Citrix-Veröffentlichung der Schwachstelle) erstellt wurden, sind verdächtig. Die Befehle der Angreifer stehen in den XML-Dateien. Die Dateien können allerdings nach einem erfolgreichen Angriff gelöscht worden sein.
Suche nach der NOTROBIN-Backdoor.	ls -latr /tmp/.init/* ls -latr /var/nstmp/.nscache/*	Weitere Indikatoren liefern [DCSO01] und [Fireeye01].
Prüfung des Bookmark-Pfads	ls -latr /var/vpn/bookmark/*.xml	Dieses Verzeichnis sollte entweder nicht existieren oder es sollten nur Dateinamen legitimer Benutzer auftauchen.

Es wird dringend empfohlen, die Citrix-Systeme durch jeweils eine Firewall in Richtung Internet und dem internen Netz zu schützen und von dem Citrix-System ein- und ausgehenden Netzverkehr restriktiv zu filtern. Dies reduziert das Risiko einer erfolgreichen Platzierung von Reverse Shells für den entfernten Zugriff durch den Angreifer und evtl. Zugriffe auf interne Netze.

Sollten Sie Hinweise auf eine Kompromittierung finden, sind folgende Maßnahmen empfohlen:

- Netztrennung der kompromittierten Citrix-Instanz.
- Sicherung der alten Citrix-Instanz (gesamtes System oder zumindest die Logdateien unter /var/log/*).

- Neuaufsetzen der Citrix-Instanz mit dem aktuellsten Build des jeweiligen Versionszweiges und Umsetzung des Workarounds.
- Erstellung neuer SSL-/TLS-Zertifikate, Zurückrufen der alten SSL-/TLS-Zertifikate.
- Zurücksetzen aller Windows Active Directory Passwörter, wenn sich der Citrix-Nutzerkreis nicht einschränken lässt.
- Je nach Netzanbindung Prüfung der Windows Domäne auf weitere Kompromittierungen.

Update 5:
Wurden auf einem kompromittierten Citrix-System Wildcard-SSL-Zertifikate (*.example.com) verwendet, sind bei dem oben angesprochenen Zertifikatstausch alle weiteren Systeme zu berücksichtigen, die das Wildcard-Zertifikat einsetzen [Twitter04], [Twitter05].

Weitere Hinweise zu der sicheren Umsetzung von Fernzugriffen stellt das BSI bereit [BSI02]-[BSI05].

Links

[BLC2020] DoppelPaymer Hacked Bretagne Télécom Using the Citrix ADC Flaw
https://www.bleepingcomputer.com/news/security/doppelpaymer-hacked-bretagne-t-l-com-using-the-citrix-adc-flaw/

[BSI01] CERT-Bund Reports
https://reports.cert-bund.de/

[BSI02] IT-Grundschutz OPS.2.4 Fernwartung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_4_Fernwartung.html

[BSI03] IT-Grundschutz NET.3.3 VPN
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html

[BSI04] Grundregeln zur Absicherung von Fernwartungszugängen v2.0
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_054.html

[BSI05] Fernwartung im industriellen Umfeld v2.0
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_108.html

[BSI06] BSI Pressemitteilung - Aktive Ausnutzung der Citrix Schwachstelle
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Citrix_Schwachstelle_160120.html

[BSI07] Ransomware: Bedrohungslage, Prävention & Reaktion
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Ransomware/ransomware_node.html

[BSI08] BSI Pressemitteilung - Cyber-Angriff auf Uniklinik Düsseldorf: BSI warnt vor akuter Ausnutzung bekannter Schwachstelle
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

[Citrix01] CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller and Citrix Gateway
https://support.citrix.com/article/CTX267027

[Citrix02] Citrix ADC (NetScaler ADC) Downloads
https://citrix.com/de-de-/downloads/citrix-adc/

[Citrix03] Citrix Gateway (NetScaler Unified Gateway) Downloads
https://citrix.com/de-de/downloads/citrix-gateway/

[Citrix04] CTX267679 - Mitigation steps for CVE-2019-19781
https://support.citrix.com/article/CTX267679

[Citrix05] Citrix Support
https://support.citrix.com/user/alerts

[Citrix06] CVE-2019-19781 – Verification Tool
https://support.citrix.com/article/CTX269180

[Citrix07] Citrix and FireEye Mandiant share forensic tool for CVE-2019-19781
https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/

[DCSO01] A Curious Case of CVE-2019-19781 Palware: remove_bds
https://blog.dcso.de/a-curious-case-of-cve-2019-19781-palware-remove_bds/

[Fireeye01] 404 Exploit Not Found: Vigilante Deploying Mitigation for Citrix NetScaler Vulnerability While Maintaining Backdoor
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html

[Fireeye02] Nice Try: 501 (Ransomware) Not Implemented
https://www.fireeye.com/blog/threat-research/2020/01/nice-try-501-ransomware-not-implemented.html

[FoxIT] A Second Look at CVE-2019-19781 (Citrix NetScaler / ADC)
https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/

[HiSolutions] Ransomware-Angriffe als Folge von Shitrix
https://www.hisolutions.com/detail/ransomware-angriffe-als-folge-von-shitrix

[Mitre] CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
https://cwe.mitre.org/data/definitions/22.html

[NCSC.NL01] Flowchart Citrix vulnerability
https://english.ncsc.nl/publications/publications/2020/januari/21/flowchart-citrix-vulnerability

[Reddit] Multiple Exploits for CVE-2019-19781 (Citrix ADC/Netscaler) released overnight - prepare for mass exploitation
https://www.reddit.com/r/blueteamsec/comments/en4m7j/multiple_exploits_for_cve201919781_citrix/

[SANS] Citrix ADC Exploits: Overview of Observed Payloads
https://isc.sans.edu/forums/diary/Citrix+ADC+Exploits+Overview+of+Observed+Payloads/25704/

[TrustedSec01] NetScaler Honeypot
https://www.trustedsec.com/blog/netscaler-honeypot/

[TrustedSec02] NetScaler Remote Code Execution Forensics
https://www.trustedsec.com/blog/netscaler-remote-code-execution-forensics/

[Twitter01] certbund
https://twitter.com/certbund/status/1214483690421727233

[Twitter02] GossiTheDog
https://twitter.com/GossiTheDog/status/1216335829125210114

[Twitter03] cyb3rops
https://twitter.com/cyb3rops/status/1215974764227039238

[Twitter04] certbund
https://twitter.com/certbund/status/1222911580230373377

[Twitter05] zentura_cp
https://twitter.com/zentura_cp/status/1222279897760124928

[Winkel] Checklist for Citrix ADC CVE-2019-19781
http://deyda.net/index.php/en/2020/01/15/checklist-for-citrix-adc-cve-2019-19781/