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. 2020-172597-1231, Version 1.2, 20.01.2020

IT-Bedrohungslage*: 2 / Gelb

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.x	~~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.x	~~Montag, 27. Januar 2020~~ Freitag, 24. Januar 2020
13.0	13.0.47.x	~~Montag, 27. Januar 2020~~ Freitag, 24. 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
10.2.6	11.1.63.x	~~Montag, 27. Januar 2020~~ Freitag, 24. Januar 2020
11.0.3	11.1.63.x	~~Montag, 27. Januar 2020~~ Freitag, 24. 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].

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.

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 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.

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].

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.

Citrix-Administratoren sollten grundsätzlich Citrix-Security-Bulletins mit Hinweisen auf neue Firmware-Versionen abonnieren, um Hinweise auf neue Firmware-Updates zu erhalten [Citrix05].

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

Links

[BSI01] CERT-Bund Repots
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

[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

[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

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

[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

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