SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

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

CSW-Nr. 2020-172597-1031, Version 1.0, 13.01.2020

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]:

Firmware-Versionszweig	Aktualisierte Build-Version	Geplantes Veröffentlichungsdatum
10.5	10.5.70.x	Freitag, 31. Januar 2020
11.1	11.1.63.x	Montag, 20. Januar 2020
12.0	12.0.63.x	Montag, 20. Januar 2020
12.1	12.1.55.x	Montag, 27. Januar 2020
13.0	13.0.47.x	Montag, 27. Januar 2020

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

* 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.

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

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 (ursprünglich ca. 4.000) [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].

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.

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].

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 [TrustedSec].

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

[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

[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/

[TrustedSec] 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