Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Citrix Application Delivery Controller (ADC)

CSW-Nr. 2023-249164-1132, Version 1.1, 16.08.2023

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 18.07.2023 wurde durch den Hersteller Citrix eine Schwachstelle in den Produkten NetScaler ADC (ehemals Citrix ADC) und NetScaler Gateway (ehemals Citrix Gateway) bekannt gegeben [CITR2023]. Die Sicherheitslücke wird gemäß Common Vulnerabilities and Exposures (CVE) unter der Nummer CVE-2023-3519 geführt und nach CVSS mit einem Score von 9.8 ("kritisch") bewertet. Demnach kann ein nicht-authentifizierter, entfernter Angreifer in die Lage versetzt werden, Code auf dem betroffenen System auszuführen. Ursache ist die Einschleusung von nicht vertrauenswürdigen Daten in eine Programmiersprache bzw. Laufzeitumgebung ("Code Injection"; CWE-94).

Gemäß der Informationen von Citrix [CITR2023] wurden bereits Angriffsversuche beobachtet. Daher empfiehlt das BSI allen betroffenen Kunden von NetScaler ADC und NetScaler Gateway, die relevanten Updates so schnell wie möglich zu installieren.

Verwundbar sind die folgenden Versionen von NetScaler ADC und NetScaler Gateway:

- NetScaler ADC und NetScaler Gateway 13.1 vor 13.1-49.13
- NetScaler ADC und NetScaler Gateway 13.0 vor 13.0-91.13
- NetScaler ADC 13.1-FIPS vor 13.1-37.159

* 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.

- NetScaler ADC 12.1-FIPS vor 12.1-55.297
- NetScaler ADC 12.1-NDcPP vor 12.1-55.297

Es ist zu beachten, dass NetScaler ADC und NetScaler Gateway Version 12.1 bereits das End-of-Life (EOL) erreicht haben und somit trotz ihrer Verwundbarkeit keine Patches erhalten.

Neben der Schwachstelle CVE-2023-3519 wurden außerdem eine Reflected Cross-Site-Scripting (CVE-2023-3466) sowie eine Privilege Escalation (CVE-2023-3467) Schwachstelle geschlossen.

Update 1:
Nach einer massiven Ausnutzung wurden annähernd 2000 Citrix NetScaler Instanzen mit Backdoors versehen. Ein Großteil der kompromittierten Server wurde zwar auf CVE-2023-3519 gepatcht, ist aber weiterhin mit einer Backdoor versehen, weil die Ausnutzung der Schwachstelle bereits vor dem Einspielen des Updates geschah [FOX2023a].

Bewertung

Die entdeckte kritische Schwachstelle (CVE-2023-3519) in den Produkten Citrix ADC und Citrix Gateway betrifft alle Geräte, die als Gateway (VPN Virtual Server, ICA Proxy, CVPN, RDP Proxy) oder Authentication Virtual Server (AAA Server) konfiguriert sind.

Application Delivery Controller stellen aufgrund ihrer Erreichbarkeit aus dem Internet und des Funktionsumfangs grundsätzlich eine große Angriffsfläche für Angreifer dar, da sie bei einer Kompromittierung den Zugriff auf Netzwerke ermöglichen.

Aufgrund der Tatsache, dass bereits Angriffsversuche auf diese Schwachstelle beobachtet wurden [CITR2023], besteht ein hohes Risiko einer Kompromittierung, wenn diese nicht umgehend behoben wird.

Update 1:
Aufgrund der schnellen großflächigen Ausnutzung ist es wahrscheinlich, dass nicht sofort aktualisierte Citrix NetScaler kompromittiert wurden. Die Gefahr vor Angreifern bleibt daher bis zur Sicherstellung, dass der Server nicht bereits eine Backdoor enthält, auch nach einem Update bestehen.

Maßnahmen

Um die Sicherheitslücke in den betroffenen Produkten NetScaler ADC und NetScaler Gateway zu beheben, sollten die verfügbaren Updates schnellstmöglichst installiert werden. Es stehen keine Workarounds zur Verfügung.

Nach Angaben des Herstellers sind die folgenden Versionsnummern (oder höher) nicht mehr durch die Schwachstelle CVE-2023-3519 verwundbar:

- NetScaler ADC und NetScaler Gateway 13.1 13.1-49.13 oder höher
- NetScaler ADC und NetScaler Gateway 13.0 13.0-91.13 oder höher
- NetScaler ADC 13.1-FIPS 13.1-37.159 oder höher
- NetScaler ADC 12.1-FIPS 12.1-55.297 oder höher
- NetScaler ADC 12.1-NDcPP 12.1-55.297 oder höher

Das BSI rät vom Einsatz von NetScaler ADC und NetScaler Gateway in Version 12.1 dringend ab, weil diese nicht mehr vom Hersteller unterstützt werden und somit verwundbar bleiben - ausgenommen die zuvor genannten Versionen FIPS bzw. NDcPP.

Für aktuelle Informationen und Hinweise zum Beheben der Schwachstelle empfiehlt das BSI IT-Sicherheitsverantwortlichen, das Advisory von Citrix [CITR2023] zu prüfen.

Des Weiteren sollte auf eine Kompromittierung geprüft werden, in dem nach Webshells bzw. Dateien gesucht wird, die neuer als das Installationsdatum sind. Zusätzlich können IT-Sicherheitsverantwortliche den HTTP-Error-Log oder Shell-Log auf Auffälligkeiten prüfen.

Da bei ADCs immer die Gefahr von Schwachstellen besteht, sollten zudem auch die getroffenen Absicherungsmaßnahmen z. B. anhand der BSI-Empfehlung [GS2020] überprüft werden.

Update 1:
IT-Sicherheitsverantwortliche sollten trotz eingespielten Updates auf eine Kompromittierung anhand von Indicators-of-Compromise (IoCs) prüfen. Es stehen Tools von FOX IT [FOX2023b] sowie Mandiant [MAND2023] auf GitHub zur Verfügung, die automatisiert auf bekannte IoCs prüfen. Shadowserver.org bietet zudem eine Liste von IoCs neben Hintergrundinformationen zu beobachteten Angriffen auf CVE-2023-3519 an [SHAD2023]. Das BSI empfiehlt auch aktualisierte Citrix NetScaler nochmals ausführlich auf eine Kompromittierung zu prüfen.

Da möglicherweise noch unbekannte Angriffe erfolgreich stattgefunden haben, sollten auch die entsprechenden Logs auf Auffälligkeiten geprüft werden (siehe u.a. [CISA2023], [SHAD2023]).

Bleiben auch nach der Prüfung Zweifel an der Integrität des Systems bestehen, kann die Inanspruchnahme externer Unterstützung in Erwägung gezogen werden. Anlaufstellen hierfür bietet zum Beispiel die Liste der vom BSI qualifizierten IT-Dienstleister [BSI2023].

Links

[CITR2023] Citrix Advisory CTX561482: Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467:
https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

[GS2020] Empfehlungen für den sicheren Einsatz von Application Delivery Controllern:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Hilfsmittel_Empfehlung_ApplicationDeliveryController_v1.pdf

Update 1:
[BSI2023] Qualifizierte Dienstleister:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html

[FOX2023a] FOX IT Approximately 2000 Citrix NetScalers backdoored:
https://blog.fox-it.com/2023/08/15/approximately-2000-citrix-netscalers-backdoored-in-mass-exploitation-campaign/

[FOX2023b] Citrix NetScaler Triage:
https://github.com/fox-it/citrix-netscaler-triage/

[MAND2023] Indicator of Compromise Scanner for CVE-2023-3519:
https://github.com/mandiant/citrix-ioc-scanner-cve-2023-3519

[SHAD2023] Technical Summary of Observed Citrix CVE-2023-3519 Incidents:
https://www.shadowserver.org/news/technical-summary-of-observed-citrix-cve-2023-3519-incidents/

[CISA2023] Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells
https://www.cisa.gov/sites/default/files/2023-07/aa23-201a_csa_threat_actors_exploiting_citrix-cve-2023-3519_to_implant_webshells.pdf

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

    TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
    Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.