

2023-031 CERT-Hessen Warnmeldung

19.07.2023, 16:00 Uhr

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

Tags: Citrix | Application Delivery Controller | Netscaler

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 Hessen3C aufgrund der Warnmeldung des BSI und der Kritikalität der Schwachstelle 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
- NetScaler ADC 12.1-FIPS vor 12.1-55.297
- NetScaler ADC 12.1-NDcPP vor 12.1-55.297

TLP-CLEAR

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.

Betroffene Produkte:

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

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.

TLP-CLEAR

Empfehlung von 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

Auf Basis der Empfehlung des BSI rät das Hessen3C 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 Hessen3C 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.

Weitere Quellen

[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

Hessen3C



TLP-CLEAR

Kurzfassung: Bedeutung der Traffic Light Protocol-Einstufungen

TLP-Stufen

Stufe	Bedeutung	Bestimmungen
TLP-White	Unbegrenzt	Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-White ohne Einschränkungen frei weitergegeben werden.
TLP-Green	Organisations- übergreifende Verteilung	Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
TLP-Amber	Organisationsinterne Verteilung	Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig“. Der Ersteller der Information muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
TLP-Red	Persönlich, nur für benannte Empfänger	TLP-Red-Informationen sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefonkonferenz bzw. auf die <u>direkten</u> Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden Informationen der Stufe TLP-Red mündlich oder persönlich übergeben.

Eine ausführliche Erläuterung zum Traffic-Light-Protokoll finden Sie im Dokument „CERT-Verpflichtung-TLP.pdf“ unter <http://www.cert.hessen.de>

Kontaktdaten:

Hessen CyberCompetenceCenter (Hessen3C)



Hessisches Ministerium des Innern und für Sport
Friedrich-Ebert-Allee 12
65185 Wiesbaden

Telefon, Sammelruf: **+49 (611) 353 9900**

Fax: +49 (611) 353 1919

E-Mail: cert@hessen3c.hessen.de

Website: <https://www.hessen3c.de>