Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Citrix NetScaler ADC und NetScaler Gateway

CSW-Nr. 2023-275276-1132, Version 1.1, 23.11.2023

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 10. Oktober 2023 hat der Hersteller Citrix ein Advisory [CITRIX23] zu Schwachstellen in den Produkten NetScaler Application Delivery Controller (ehemals Citrix ADC) und NetScaler Gateway (ehemals Citrix Gateway) veröffentlicht.Die eine kritische Sicherheitslücke wird gemäß Common Vulnerabilities and Exposures (CVE) unter der NummerCVE-2023-4966 geführt und nach CVSS mit einem Score von 9.4 ("kritisch") bewertet. Die Schwachstelle erlaubt Angreifenden sensible Informationen ohne Authentifizierung offenzulegen. Dies ermöglicht es authentifizierte Sessions zu übernehmen ("Session Hijacking") und Multifaktoren-Authentifikation (MFA) oder andere Authentifizierungsmittel zu umgehen.

Das IT-Sicherheitsunternehmen Mandiant hat einen Blogbeitrag am 17. Oktober veröffentlicht. In diesem wird angegeben, dass eine erste **Ausnutzung der Schwachstelle CVE-2023-4966** identifiziert wurde, die **bereits Ende August 2023** stattfand. [MAND23a]

Angreifende können mit authentifizierten Sessions weitere Zugangsdaten sammeln und sich somit möglicherweise höhere Rechte verschaffen und im System sowie Netzwerk ausbreiten. Eine Ausnutzung wurde von Mandiant in Dienstleistungs- und Technologie-Unternehmen sowie bei Regierungs-Organisationen beobachtet. [MAND23a]

* 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.

Betroffen von den Schwachstellen sind alle NetScaler ADC und Gateway Systeme, die als Gateway (VPN Virtual Server, ICA Proxy, CVPN, RDP Proxy) oder AAA Virtual Server konfiguriert wurden und folgende Patchstände aufweisen [CITRIX23]:

- NetScaler ADC und NetScaler Gateway 14.1 vor 14.1-8.50
- NetScaler ADC und NetScaler Gateway 13.1 vor 13.1-49.15
- NetScaler ADC und NetScaler Gateway 13.0 vor 13.0-92.19
- NetScaler ADC 13.1-FIPS vor 13.1-37.164
- NetScaler ADC 12.1-FIPS vor 12.1-55.300
- NetScaler ADC 12.1-NDcPP vor 12.1-55.300

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.

Update 1:
Die Cybersecurity and Infrastructure Security Agency (CISA) veröffentlichte am 21.11.2023 einen umfassenden Analysebericht mit weiteren Indicators of Compromise (IoCs) zu der oben genannten Schwachstelle.

In diesem Bericht wird von vier Dateien gesprochen, die CISA für die Analyse erhalten hat. Diese Dateien zeigen unter anderem, dass Registrierungsschlüssel erstellt wurden, der Arbeitsspeicher des Local Security Authority Subsystem Service (LSASS) auf die Festplatte geschrieben wurde und Versuche unternommen wurden, Sitzungen über das Windows Remote Management (WinRM) zu etablieren. Die Dateien enthielten unter anderem: Windows Batch (.bat)-, Windows Executable (.exe)-, Windows Dynamic Link Library (.dll)- und Python Script (.py)-Dateien.

Weitere umfassende Informationen zu dem Analysebericht, den IoCs und YARA-Regeln zur Detektion können hier entnommen werden [CISA2023].

Bewertung

Application Delivery Controllerstellen aufgrund ihrer Erreichbarkeit aus dem Internet und des Funktionsumfangsgrundsätzlich eine große Angriffsfläche für Angreifer dar, da sie bei einer Kompromittierung den Zugriff auf Netzwerkeermöglichen.

Aufgrund der Tatsache, dass bereits seit Ende August eine Ausnutzung der Schwachstelle (CVE-2023-4966) beobachtet wurde [MAND23a], besteht ein hohes Risiko einer bereits stattgefundenen Kompromittierung.

Auch wenn die Schwachstelle lediglich das Entwenden bzw. Hijacken von Session-Informationen für den NetScaler ADC und NetScaler Gateway und damit das Umgehen der Authentifizierung erlaubt, so können Angreifende damit Zugangsdaten entwenden und sich auf weitere Systeme in der Umgebung ausbreiten.

Maßnahmen

IT-Sicherheitsverantwortliche sollten zum Beheben der Sicherheitslücken in den betroffenen Produkten NetScaler ADC und NetScaler Gateway dieverfügbaren Updates schnellstmöglich installieren.

Folgende Versionen von NetScaler ADC und NetScaler Gateway beheben die Schwachstelle und sollten installiert werden [CITRIX23]:

- NetScaler ADC und NetScaler Gateway 14.1-8.50 oder höher
- NetScaler ADC und NetScaler Gateway 13.1-49.15 oder höhere Versionen von 13.1
- NetScaler ADC und NetScaler Gateway 13.0-92.19 oder höhere Versionen von 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.164 oder höhere Versionen von 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.300 oder höhere Versionen von 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.300 oder höhere Versionen von 12.1-NDcPP

Solange keine Patches installiert sind, sollte der Zugriff auf NetScaler Instanzen nur auf vertrauenswürdige Netze beschränkt werden, um keine Angriffsfläche aus dem Internet zu bieten.

Es ist möglich, dass selbst nach einem eingespielten Update, die von Angreifenden genutzten authentifizierten Sessions weiterhin gültig sind. **Daher ist es notwendig nach dem Installieren des Updates alle aktiven und persistenten Sessions auf den Instanzen zu terminieren.**

Hierzu kann sich mit der entsprechenden NetScaler Instanz verbunden werden und mittels des Command Line Interfaces und des Befehls

> *clear lb persistentSessions <vServer>*

wobei <*vServer*> mit dem Namen des Virtual Servers bzw. Appliance ausgetauscht werden muss, können persistente Sessions terminiert werden. [MAND23b]

Es ist empfehlenswert alle verbundenen Zugangsdaten, die im Zusammenhang mit der NetScaler Instanz stehen, auszutauschen. Aufgrund des Fehlens von Log Einträgen, die eine Ausnutzung aufzeigen könnten, kann diese nicht auf den NetScaler Systemen detektiert werden. Sollten verdächtige Aktivitäten im Netzwerk beobachtet werden, sollten die Zugangsdaten schnellst möglichst ausgetauscht werden, vor allem, wenn Zugang zu den Systemen mit verdächtigen Aktivitäten aus dem Internet besteht. [MAND23b]

NetScaler ADCs oder NetScaler Gateways auf denen WebShells oder andere Backdoors gefunden wurden, sollten mittels eines Source-Image neu aufgesetzt werden, ggf. einspielbare Backups sind auf eine bereits enthaltende Backdoor zu prüfen. Sollte eine Web Application Firewall (WAF) oder andere Systeme vor dem NetScaler System sein, das URL Anfragen loggt, so können diese auf viele Anfragen von verdächtigen Quellen (IPs) untersucht werden. [MAND23b]

Zur Absicherung von ADCs können die Empfehlungen vom BSI zum sicheren Einsatz solcher Systeme [GS2020] umgesetzt werden.

Links

[CITRIX23] Citrix NetScaler ADC und Gateway Advisory

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

[MAND23a] Remediations for Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966)

https://www.mandiant.com/resources/blog/remediation-netscaler-adc-gateway-cve-2023-4966

[MAND23b] Citrix NetScaler ADC / Gateway: CVE-2023-4966 Remediation

https://services.google.com/fh/files/misc/citrix-netscaler-adc-gateway-cve-2023-4966-remediation.pdf

[GS2020]Empfehlungen für den sicheren Einsatz vonApplication Delivery Controllern

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Hilfsmittel_Empfehlung_ApplicationDeliveryController_v1.pdf

Update 1:
[CISA2023] CISA Malware Analysis Report Citrix Bleed (CVE-2023-4966)

https://www.cisa.gov/news-events/analysis-reports/ar23-325a

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.