WATCHTOWER

Threat Intelligence Report

Citrix ADC & NetScaler Gateway kwetsbaarheden (CVE-2023-3519)

Datum: 18/07/2023
Versie: 1.0

Publieke versie

bsi ISO/IEC 27001 Information Security Management CERTIFIED

NFIR

Beschrijving dreigingsbeeld

Op 18 juli 2023 heeft het NFIR TI Watchtower-team informatie verzameld over het dreigingsbeeld inzake de kwetsbaarheid met CVE-nummer CVE-2023-3519.

Specifiek inzake de dreiging waarin een actor misbruik maakt van een kwetsbaarheid in Citrix ADC / NetScaler Gateway. Deze kwetsbaarheid stelt een aanvaller in staat om toegang te verkrijgen tot de getroffen systemen en achterliggende doelsystemen door het uitvoeren van malafide code.

Citrix meldt dat de kwetsbaarheid met kenmerk CVE-2023-3519 actief wordt misbruikt. Voor het succesvol misbruiken van de kwetsbaarheid is het vereist dat het kwetsbare systeem als Gateway (VPN-virtual server, ICA Proxy, CVPN, RDP Proxy) of als AAA virtual server geconfigureerd is.

De volgende versies van Citrix ADC / NetScaler Gateway zijn volgens Citrix[1] kwetsbaar voor misbruik:

Product	Platform	CVSS-score
• NetScaler ADC en NetScaler Gateway 13.1 voor versie 13.1-49.13 • NetScaler ADC en NetScaler Gateway 13.voor versie 13.0-91.13 • NetScaler ADC 13.1-FIPS voor versie 13.1-37.159 • NetScaler ADC 12.1-FIPS voor versie 12.1-55.297 • NetScaler ADC 12.1-NDcPP voor versie 12.1-55.297 **Opmerking: NetScaler ADC en NetScaler Gateway versie 12.1 is nu End Of Life (EOL) en blijft kwetsbaar.**	NetScaler ADC NetScaler Gateway	9.8– Kritiek

Tabel 1: Overzicht van de getroffen producten

De volgende CVSS-vector string is door Citrix toegewezen aan de kwetsbaarheid:

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NFIR adviseert aan organisaties die Citrix-producten gebruiken (specifiek Citrix ADC / NetScaler Gateway) om vast te stellen of de kwetsbare versies van Citrix ADC / NetScaler Gateway zoals hierboven beschreven aanwezig zijn op systemen binnen uw organisatie.

Indien er een kwetsbare versie geconstateerd wordt, adviseert NFIR om een (forensisch) kopie of snapshot van de machine te maken en aansluitend de software-versie te updaten. Indien er indicaties zijn van mogelijk misbruik door actoren adviseert NFIR om forensisch onderzoek en/of incident response uit te laten voeren.

> Acuut hulp nodig? Bel dan onze 24/7 CERT-lijn via 088 133 0700 en wij doen ons uiterste best om u zo snel mogelijk te helpen.

[1] https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Actieplan

Het is belangrijk voor organisaties welke gebruik maken van Citrix ADC / NetScaler Gateway om ten minste de volgende stappen te nemen:

1. Indien uw organisatie gebruikmaakt van Citrix ADC / NetScaler Gateway om vast te stellen of uw systemen kwetsbaar zijn. Controleer hiervoor de Citrix ADC / NetScaler Gateway-versie van de aanwezige (virtuele) systemen binnen uw netwerkomgeving;
2. Indien uw systemen kwetsbaar zijn adviseert NFIR om de getroffen systemen te updaten naar versies welke niet langer kwetsbaar zijn;
3. Indien er indicaties zijn dat uw systemen misbruikt zijn adviseert NFIR om forensisch onderzoek uit te laten voeren om vast te stellen of uw omgeving gecompromitteerd is.
4. Controleer (indien beschikbaar) publiek beschikbare Indicators-of-Compromise (IoC's) op uw systemen om vast te stellen of er systemen mogelijk gecompromitteerd zijn, of laat extern preventief onderzoek uitvoeren naar uw systemen;

Zijn systemen kwetsbaar en zijn er systemen waarvan het risico groot is (bijvoorbeeld systemen met zeer gevoelige of bijzondere persoonsgegevens)? Zo ja, heeft u mogelijke indicaties dat het systeem niet direct gemitigeerd en/of geüpdatet kan worden? Overweeg dan om het systeem tijdelijk uit te schakelen totdat deze geüpdatet kan worden.

TTPs – CVE-2023-3519

Tactics, Techniques and Procedures (TTPs) gerelateerd aan handelingen van CVE-2023-3519 zoals waargenomen bij NFIR Watchtower zijn als volgt:

Initial Access

- T1190 - Exploit Public-Facing Application

Execution

- T1059 - Command and Scripting Interpreter
- T1059.003 - Windows Command Shell
- T1059.004 -Unix Shell

Persistence

- T1505.003 - Server Software Component: Web Shell

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren, incident responders die u helpen om aanvallen te mitigeren en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

Gespecialiseerd in

- Het verzamelen, identificeren en valideren van digitale informatie
- Onderzoek naar computers, servers, e-mailverkeer, gegevensdragers, websites en personen

Multidisciplinair onderzoek

- Sporen en gegevens verzamelen en reconstrueren
- Heldere rapportage bruikbaar voor juridische procedures en andere officiële instanties

Samenwerking met

- Tactisch rechercheurs, privacy juristen, gerechtsdeurwaarders, Politie, NCSC, IBD, het Openbaar Ministerie en internationale diensten.

NFIR als adviseur Forensisch Onderzoek

- Samen met de opdrachtgever wordt de scope van het onderzoek bepaald
- Praktisch toepasbare adviezen na afronding van het onderzoek

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl