NFIR Threat Intelligence Report

Kritieke kwetsbaarheden in Citrix Gateway & Citrix Application Delivery Controller (ADC) - CVE-2022-27510

Datum: 9/11/2022

Versie: 1.0

bsi ISO/IEC 27001 Information Security Management CERTIFIED

NFIR

Beschrijving

Op 8 november 2022 is er een advisory gepubliceerd[1] door het Citrix voor de producten Citrix Gateway en Citrix ADC inzake een drietal kwetsbaarheden waarvan een kwetsbaarheid (CVE-2022-27510) de CVSS-classificatie classificatie “Kritiek” draagt.

Wat zijn Citrix Gateway / ADC?

Citrix Applicaton Delivery Controller, ofwel ADC (het vroegere NetScaler ADC) is een oplossing voor application delivery en load balancing. Het wordt gebruikt voor het faciliteren van applicaties binnen bedrijfsomgevingen. Citrix Gateway is een on-premise oplossing die remote access faciliteert en de toegang tot apps en resources verschaft.

De getroffen producten betreffen volgens Citrix tenminste de volgende producten:

CVE-nummer	Product	CVSS-Classificatie
CVE-2022-27510	Citrix ADC & Citrix Gateway 13. voor sub-versie .1-33.47 Citrix ADC & Citrix Gateway 13. voor sub-versie .0-88.12 Citrix ADC & Citrix Gateway 12. voor sub-versie .1.65.21 Citrix ADC 12.1-FIPS voor versie 12.1-55.289 Citrix ADC 12.1-NDcPP voor versie 12.1-55.289	Kritiek

Tabel 1: Overzicht van de getroffen producten

Het Nederlandse Nationaal Cyber Security Centrum (NCSC-NL)[2] heeft daarnaast een aanvullende advisory gepubliceerd.

Publieke exploits

Er zijn op het moment van schrijven **nog geen publieke** exploits beschikbaar voor de beschreven kwetsbaarheden. NFIR schat het risico op eventueel misbruik in de toekomst als **reëel** in.

Aanbeveling

NFIR adviseert aan getroffen klanten van Citrix ADC en Citrix Gateway om de relevante bijgewerkte versies van Citrix ADC of Citrix Gateway zo snel mogelijk te installeren:

- Citrix ADC en Citrix Gateway 13.1-33.47 en latere versies
- Citrix ADC en Citrix Gateway 13.0-88.12 en latere versies van 13.0
- Citrix ADC en Citrix Gateway 12.1-65.21 en latere versies van 12.1
- Citrix ADC 12.1-FIPS 12.1-55.289 en latere versies van 12.1-FIPS
- Citrix ADC 12.1-NDcPP 12.1-55.289 en latere versies van 12.1-NDcPP

[1] https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516
[2] https://advisories.ncsc.nl/advisory?id=NCSC-2022-0701

Mogelijke Impact

Als een aanvaller in staat is om de kwetsbaarheid succesvol uit te buiten, dan kan dit leiden tot ongeautoriseerde toegang tot Citrix-systemen, alsmede achterliggende systemen die onderdeel zijn van de netwerk-infrastructuur.

Om deze kwetsbaarheid te misbruiken moet het systeem zijn ingesteld als Gateway waarbij gebruik wordt gemaakt van de SSL VPN functionaliteit of als het systeem is geconfigureerd als ICA proxy met authenticatie. Citrix schaalt de kwetsbaarheid in als "critical".

> NFIR **adviseert** u om forensisch onderzoek te laten doen naar of uw systemen getroffen zijn.

Actieplan

Het is belangrijk voor uw organisatie om ten minste de volgende stappen te nemen:

1. Controleer (indien beschikbaar) de 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.
2. Bereid uw organisatie voor op de situatie dat er onverwacht patches uitgevoerd dienen te worden (buiten de reguliere update-timeframes) en pas patches gecontroleerd toe volgens de voor uw organisatie gebruikelijke procedure.
3. Voer de beschikbare beveiligingsupdates/patches, zodra deze gepubliceerd zijn, direct uit op de systemen en verifieer of de updates daadwerkelijk toegepast zijn. In het geval dat u een externe IT-dienstleverancier heeft: Laat uw leverancier deze handelingen uitvoeren en laat deze de handelingen en het resultaat hiervan schriftelijk aan u bevestigen.

Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met zeer gevoelige of bijzondere persoonsgegevens)? Zo ja, heeft u mogelijk 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.

Wat moet uw organisatie doen bij mogelijk misbruik?

Als uw organisatie vermoedelijk het slachtoffer is geworden van een aanval, is het dringende advies om onderzoek uit te laten voeren naar de toedracht, in hoeverre aanvallers mogelijk andere systemen hebben gecompromitteerd en welke informatie mogelijk ongeautoriseerd geraadpleegd is.

1. Koppel indien mogelijk de getroffen systemen los van het netwerk, maar laat deze aanstaan (in verband met eventuele sporen zoals het vluchtige geheugen – RAM);
2. Laat de getroffen systemen forensisch onderzoeken; zorg voor adequate back-ups;
3. Reset uw wachtwoorden en gebruikersgegevens;
4. Doe aangifte bij de Politie;
5. Overweeg een melding te doen bij de Autoriteit Persoonsgegevens.

Heeft uw organisatie op dit moment een incident? Onze Computer Emergency Response Teams (CERT) staan 24/7 voor organisaties klaar om te ondersteunen bij IT- Security Incidenten.

Bel dan 088 133 0700 en wij doen ons uiterste best om u zo snel mogelijk te helpen. (Meer informatie over onze Incident Response Dienst.)

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 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