WATCHTOWER

Threat Intelligence Report

ShareFile Remote Code Execution (CVE-2023-24489)

Datum: 17/07/2023
Versie: 1.2

Publieke versie

bsi ISO/IEC 27001 Information Security Management CERTIFIED

NFIR

Beschrijving dreigingsbeeld

Op 17 juli 2023 het NFIR TI Watchtower-team aanvullende informatie verzameld over het dreigingsbeeld inzake de kwetsbaarheid met CVE-nummer CVE-2023-24489. Dit omdat er inmiddels publieke exploits beschikbaar zijn.

Specifiek inzake de dreiging waarin een actor misbruik maakt van een kwetsbaarheid in Citrix ShareFile en Content Collaboration. Deze kwetsbaarheid stelt een aanvaller in staat om toegang te verkrijgen tot de getroffen systemen en achterliggende doelsystemen.

Citrix ShareFile en Content Collaboration wordt door organisaties gebruikt voor het samenwerken, delen en synchroniseren van inhoud horende bij documenten en workflows.

De volgende versies van Citrix ShareFile/ Content Collaboration zijn volgens Citrix[1] kwetsbaar voor misbruik:

Product	Platform	CVSS-score
Citrix ShareFile / Content Collaboration - Lager dan versie 5.11.24	Citrix ShareFile / Content Collaboration	9.8– Kritiek

Tabel 1: Overzicht van de getroffen producten

De volgende CVSS-vector string is door NIST toegewezen is aan de kwetsbaarheid[2]:

- 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 ShareFIle / Content Collaboration) om vast te stellen of de kwetsbare versies van ShareFile / Content Collaboration zoals hierboven beschreven aanwezig zijn op systemen binnen uw organisatie.

Indien er een kwetsbare versie geconstateerd wordt, adviseert NFIR om deze software-versie te updaten en indien er indicaties over misbruik door actoren aanwezig zijn om forensisch onderzoek en/of incident response uit te laten voeren om te achterhalen of er sporen van misbruik van de kwetsbaarheid zijn.

> 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/CTX559517/sharefile-storagezones-controller-security-update-for-cve202324489
[2] https://nvd.nist.gov/vuln/detail/CVE-2023-24489

Actieplan

Het is belangrijk voor organisaties welke gebruik maken van Citrix ShareFile / Content Collaboration om ten minste de volgende stappen te nemen:

1. Indien uw organisatie gebruikmaakt van ShareFile / Content Collaboration om vast te stellen of uw systemen kwetsbaar zijn. Controleer hiervoor de ShareFile / Content Collaboration-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 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.

Indicators of Compromise (IoCs) gerelateerd aan CVE-2023-24489

TTPs gerelateerd aan handelingen van CVE-2023-24489 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

C2-behavior

- T1105 - Ingress Tool Transfer

Indicatoren gerelateerd aan CVE-2023-24489:

Type	Waarde	Beschrijving
Uitvoerbaar bestand	/usr/bin/mono	Gebruikte Living Of the Land binary (LOLBIN)
Uitvoerbaar bestand	cmd.exe	Gebruikte Living Of the Land binary (LOLBIN)
Gebruiker/Security Identifier	nt system\authority (S-1-5-18)	Gebruiker misbruikt via exploit (Windows)
Gebruiker	root	Gebruiker misbruikt via exploit (Unix)
Bestandspad	/cifs/x.aspx	Backdoor (ASPX)
Bestandspad	/cifs/real.aspx	Backdoor (ASPX)
URL	https://CUSTOMER/cifs/real.aspx	Backdoor URL (ASPX)
URL	https://CUSTOMER/cifs/x.aspx	Backdoor URL (ASPX)

Table 1 - Indicatoren handelingen CVE-2023-24489

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