NFIR Threat Intelligence Report

Patches beschikbaar voor kritieke kwetsbaarheden in Microsoft Windows besturingssystemen - CVE-2022-26809 en CVE-2022-24491

Datum: 13/04/2022
Versie: 1.0

Beschrijving

Op dinsdag 12 april 2022 heeft Microsoft patches voor meerdere kwetsbaarheden gepubliceerd.

De specifieke kwetsbaarheden waarvoor dit Threat Intelligence Report geschreven is zijn de kwetsbaarheden (CVE-2022-26809/ CVE-2022-24491) waarmee het voor een aanvaller mogelijk is om zonder te authentiseren malafide code uit te voeren op de getroffen systemen.

De getroffen producten betreffen volgens CERT-EU[1] Microsoft Windows producten van tenminste Windows-OS versie 7 tot en met Windows Server 2022.

Hieronder is een overzicht opgenomen van de specifieke kwetsbaarheden:

CVE-nummer	Beschrijving	CVSS3.1-score
CVE-2022-26809	RPC Runtime Library Remote Code Execution Vulnerability (RCE)	9.8
CVE-2022-24491	Windows Network File System Remote Code Execution Vulnerability	9.8

Tabel 1: Overzicht van de kwetsbaarheden

Gezien de ernst van deze kwetsbaarheden adviseert NFIR om de beschikbaar gestelde patches zo snel mogelijk te installeren.

CVE-2022-26809 - RPC Runtime Library Remote Code Execution Vulnerability (RCE)

Door gebruik te maken van een speciaal voorbereid Remote Procedure Call (RPC)-verzoek, kan een aanvaller malafide code uitvoeren met dezelfde rechten als de RPC-service op het systeem dat aangevallen wordt.

Deze kwetsbaarheid is geclassificeerd als **wormable**, wat betekent dat de kwetsbaarheid zich kan verspreiden naar andere kwetsbare systemen zonder enige interactie.

CVE-2022-24491- Windows Network File System Remote Code Execution Vulnerability

De tweede kwetsbaarheid stelt een aanvaller, net als de eerste kwetsbaarheid, in staat om malafide code uit te voeren op het getroffen systeem.

Daarbij kunnen systemen waarbij de Network File System (NFS)-rol ingeschakeld is het doelwit worden van een aanval waarbij een speciaal voorbereid NFS-verzoek verstuurd wordt.

Dit leidt ertoe dat een aanvaller op afstand code kan uitvoeren op de getroffen machine zonder enige interactie. Ook deze kwetsbaarheid wordt daarom beschouwd als **wormable**.

[1] https://media.cert.europa.eu/static/SecurityAdvisories/2022/CERT-EU-SA2022-026.pdf

Mogelijke Impact

Als een aanvaller in staat is om de kwetsbaarheid succesvol uit te buiten dan kan dit leiden tot het uitvoeren van ongeautoriseerde code op de getroffen systemen. Dit kan mogelijk er in resulteren dat de server en de aanwezige data gecompromitteerd raakt. Deze aanval kan uitgevoerd worden vanaf het internet waarbij geen authenticatie vereist is.

Vanuit een gecompromitteerde server kan een aanvaller mogelijk toegang verkrijgen tot de rest van het netwerk. Om deze reden is de CVSS-score[2] van de kwetsbaarheden geclassificeerd als **kritiek** (9.8).

Legenda CVSS-scores

Classificatie	Score
Kritiek	9.0 – 10.0
Hoog	7.0 – 8.9
Gemiddeld	4.0 – 6.9
Laag	0.1 – 3.9
Informatief	0.0

Tabel 2: CVSS-scores

Publieke exploits

Er zijn momenteel nog geen publieke exploits beschikbaar voor de twee beschreven kwetsbaarheden, maar de verwachting is wel dat deze binnenkort beschikbaar komen. Mede doordat deze kwetsbaarheden voor aanvallers zeer relevant zijn om toegang te kunnen verkrijgen tot systemen, schat NFIR het risico op eventueel misbruik als **zeer reëel** in.

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809; https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491

Aanbeveling

NFIR adviseert om zo snel als mogelijk de betrokken systemen te voorzien van de door Microsoft beschikbaar gestelde beveiligingsupdates:

- CVE-2022-26809 - Security Update Guide - Microsoft - Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2022-24491 - Security Update Guide - Microsoft - Windows Network File System Remote Code Execution Vulnerability
- April 2022 Security Updates - Release Notes - Security Update Guide - Microsoft

Op het moment dat het toepassen van de beveiligingsupdates (nu) niet mogelijk is, kunnen de volgende mitigaties toegepast worden:

CVE-2022-26809

1. Poort 445 wordt zeer waarschijnlijk gebruikt om de RPC-verbinding op te zetten en de kwetsbaarheid te kunnen misbruiken. Door deze poort te blokkeren in de firewall (netwerk-perimeter) wordt (een beperkte vorm van) detectie/bescherming geboden tegen pogingen van buitenaf om deze kwetsbaarheid uit te buiten. Systemen kunnen echter nog steeds kwetsbaar zijn voor aanvallen vanuit het interne netwerk, waardoor misbruik van deze kwetsbaarheid zich snel binnen een netwerk kan verspreiden.

CVE-2022-24491

1. De kwetsbaarheid kan zeer waarschijnlijk alleen worden uitgebuit op systemen waar de Network File System (NFS)-rol ingeschakeld staat. Het uitbuiten kan worden voorkomen door deze rol uit te schakelen. Meer informatie over het uitschakelen van Windows-rollen kan hier worden gevonden: https://docs.microsoft.com/en-us/windows-server/administration/server-manager/install-or-uninstall-roles-role-services-or-features#install-roles-role-services-and-features-by-using-the-add-roles-and-features-wizard

Voor diensten van derden die u gebruikt, adviseert NFIR u om contact op te nemen met de leverancier voor de bevestiging dat eventuele updates toegepast zijn.

Actieplan

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

1. 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.
2. Voer de beschikbare beveiligingsupdates/patches uit op de systemen en verifieer of de updates daadwerkelijk toegepast zijn - In het geval van externe IT-dienstleverancier: Laat uw leverancier deze handelingen uitvoeren en laat deze handelingen en het resultaat hiervan schriftelijk aan u bevestigen.

Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met gevoelige of bijzonder persoonsgegevens)? Zo ja heeft u mogelijk indicaties dat het systeem niet direct 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