NFIR Threat Intelligence Report

Nieuwe kwetsbaarheden in Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082) ProxyNotShell

Datum: 02/01/2023
Versie: 1.1

Beschrijving

Op 29 september 2022 is een blog gepubliceerd door GTSC, een Vietnamees security bedrijf, dat twee nieuwe kwetsbaarheden in Microsoft Exchange Server zijn geconstateerd en misbruikt zijn bij een beperkt aantal organisaties. [1]

Deze kwetsbaarheden worden op het moment van schrijven 2 januari 2023 nog steeds misbruikt door hackers op omgevingen die nog steeds niet gepatched zijn..

Historie van deze kwetsbaarheden:
Microsoft heeft in de ochtend van 30 september 2022 (Europese tijdszones) in het Microsoft Security Response Center een 'Customer Guidance' artikel gepubliceerd waarin Microsoft bevestigt twee gerapporteerde zero-day kwetsbaarheden te onderzoeken. Het betreft CVE-2022-41040, een Server-Side Request Forgery (SSRF) kwetsbaarheid en CVE-2022-41082, een RCE (Remote Code Execution) kwetsbaarheid indien PowerShell toegankelijk is voor de aanvaller.

Microsoft is op de hoogte van beperkte gerichte aanvallen waarbij de kwetsbaarheden worden misbruikt om in de systemen van slachtoffers te komen. Bij deze aanvallen kan CVE-2022-41040 een 'authenticated' aanvaller (de aanvaller moet dus al beschikken over een succesvolle geslaagde login op de betreffende omgeving) in staat stellen om vervolgens CVE-2022-41082 te activeren. Opgemerkt dient te worden dat geauthenticeerde toegang tot de kwetsbare Exchange Server nodig is om één van de twee kwetsbaarheden met succes uit te buiten. De kwetsbaarheid maakt gebruik van de zogenaamde Autodiscover functionaliteit. URL's die gebruik maken van Autodiscover hebben geen Multi-Factor Authenticatie (MFA) bescherming.

Deze kwetsbaarheden lijken erg op kwetsbaarheden die vorig jaar werden gemeld, genaamd ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207). De kwetsbaarheid is in de cybersecurity gemeenschap (zie Twitter @GossiTheDog) bestempeld als **#ProxyNotShell**.

Update 2 januari 2023

Microsoft heeft 8 november 2022 security updates gereleased voor Exchange Server 2013, 2016 en 2019. Deze beschermen tegen CVE-2022-41040 en CVE-2022-41082. NFIR beveelt ten allen tijde aan zo snel mogelijk patches te installeren zodra ze beschikbaar zijn. Deze patches vormen de structurele definitieve maatregel en overrulen de tijdelijke mitigerende maatregelen. Zie ook de FAQ sectie in het Microsoft blog:

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2022-exchange-server-security-updates/ba-p/3669045

Voor omgevingen die nog kwetsbaar zijn voor CVE-2022-41040 en CVE-2022-41082 worden door security researchers regelmatig nieuwe exploits gepubliceerd. Zie bijvoorbeeld dit artikel van 20 december 2022 van CrowdStrike:

OWASSRF: CrowdStrike Identifies New Method for Bypassing ProxyNotShell Mitigations

[1] https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

Dit betekent dat de tijdelijke maatregelen die als workaround gepubliceerd zijn in 2022 niet meer voldoende zijn om deze CVE kwetsbaarheden te dichten. Exchange up to date houden met de meest recente patches van Microsoft is het devies. De aanbeveling is om minimaal patch level November 2022 te hebben voor Exchange Server ter bescherming tegen CVE-2022-41040 en CVE-2022-41082.

Update 3 oktober 2022

Microsoft heeft een update gepubliceerd van het 'Customer Guidance'artikel.

- Een script kan gebruikt worden om mitigerende maatregelen geautomatiseerd uit te voeren, zie https://microsoft.github.io/CSS-Exchange/Security/EOMTv2/
- Aanvullende informatie over detectie mogelijkheden zijn toegevoegd
- De aanbeveling over dichtzetten Remote Powershell is gewijzigd in instructies om remote PowerShell uit te schakelen voor gebruikers die geen beheerder zijn, zie https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers?view=exchange-ps%22%20\l%20%22use-the-exchange-management-shell-to-enable-or-disable-remote-powershell-access-for-a-user
- NFIR beveelt aan om de 'Customer Guidance' van Microsoft regelmatig te checken op updates. Het is aannemelijk dat security researchers nieuwe 'bypasses' vinden om de mitigerende maatregelen te omzeilen. Als reactie daarop is het aannemelijk dat Microsoft aanvullende verbeterde mitigerende maatregelen zal publiceren.
- De link naar het Customer Guidance artikel is ongewijzigd (de inhoud is ge-updated) en vindt u hier: https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Tekst Originele publicatie 30 september 2022

Tot er een patch is, is het sterk aanbevolen om de richtlijnen te volgen voor mitigatie en detectie om klanten te helpen zichzelf tegen deze aanvallen te beschermen.

Microsoft Exchange Online heeft al detectie en mitigatie om klanten te beschermen. Alleen omgevingen met Microsoft Exchange Server (on-premise of hybride) zijn mogelijk kwetsbaar.

De getroffen producten betreffen volgens Microsoft tenminste de volgende producten:

CVE-nummer	Product
CVE-2022-41040	Microsoft Exchange Server • Server 2013, 2016, 2019
CVE-2022-41082	Microsoft Exchange Server • Server 2013, 2016, 2019

Tabel 1: Overzicht van de getroffen producten

Op het moment van schrijven 30 september 2022 zijn volgens Microsoft alle versies van Exchange Server **kwetsbaar** (lopende het Microsoft onderzoek) en zijn er nog geen patches gepubliceerd. [2]

Publieke exploits

Er zijn op het moment van schrijven **nog geen publieke** exploits beschikbaar voor de beschreven kwetsbaarheden. Echter, de verwachting is dat deze op **zeer korte** termijn beschikbaar komen doordat deze kwetsbaarheden voor aanvallers zeer interessant zijn om (verder) toegang te kunnen verkrijgen tot systemen. NFIR schat het risico op eventueel misbruik als **reëel** in.

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 erin resulteren dat de server en de aanwezige data gecompromitteerd raakt. Deze aanval kan uitgevoerd worden vanaf het internet waarbij authenticatie vereist is.

Vanuit een gecompromitteerde server kan een aanvaller mogelijk toegang verkrijgen tot de machine en mogelijk tot de rest van het netwerk.

Workarounds

Op het moment van schrijven zijn er geen patches gepubliceerd door Microsoft – wel zijn er een aantal workarounds beschreven door Microsoft:

Mitigatie 1: Blokkeer in IIS Manager zogenaamde Autodiscover URL's op basis van de nu bekende URL patronen; zie hiervoor de instructies gepubliceerd door Microsoft [3].

Mitigatie 2: Blokkeer de poorten die gebruikt worden door 'Remote PowerShell'.
Dit betreft HTTP: 5985 en HTTPS: 5986.

Mitigatie 3: Indien er überhaupt geen noodzaak is voor het op internet beschikbaar stellen van Outlook Web Access (OWA); blokkeer OWA in het geheel.

Voor diensten van derden die u gebruikt, adviseert NFIR u om contact op te nemen met de leverancier zodat, zodra de patches beschikbaar zijn, deze kunnen worden toegepast.

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

[2] https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
[3] https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Detectie

Microsoft heeft in de 'Customer Guidance' rapportage een aantal concrete mitigerende maatregelen opgenomen.[4] NFIR beveelt ten zeerste aan deze maatregelen uit te voeren.

Indien u niet weet of u kwetsbare Outlook Web App services beschikbaar stelt op internet kunt u op Shodan.io website zoeken met:

```
http.component:"outlook web app" en door de filter toe te voegen
org:uworganisatienaam of ssl:"*uworganisatienaam"
```

Actieplan

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

1. Controleer 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. Voer de beschikbaar gestelde workarounds uit om, waar mogelijk, de impact te beperken.
3. 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.
4. 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.

[4] https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

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