aDvens

Security for the greater good

Newscast

Zero day Microsoft Exchange

Sommaire

1. Microsoft Exchange Zero day

1.1. Deux vulnérabilités détectées

La société vietnamienne de cybersécurité GTSC alerte dans son article du 28 septembre, de l'existence et l'exploitation de deux vulnérabilités impactant les serveurs **Microsoft Exchange 2013, 2016 et 2019**.

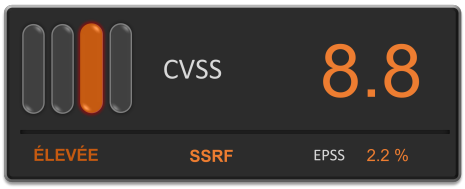

Figure 1. CVE-2022-41040

La première vulnérabilité référencée comme CVE-2022-41040, est de type Server-side Request Forgery (SSRF).

Elle permet à un attaquant d'interagir avec le serveur, afin d'en extraire des fichiers, de trouver d'autres services actifs et de cartographier le réseau interne.

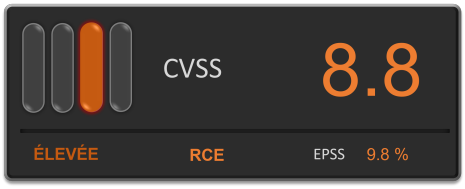

Figure 2. CVE-2022-41082

La seconde, référencée comme CVE-2022-41082, permet à un attaquant qui accède au *Powershell d'Exchange* d'exécuter du code à distance (RCE).

Ces vulnérabilités ne peuvent être exploitées uniquement si l'attaquant est authentifié sur le serveur.

Utilisées conjointement, ces failles permettraient de déployer des web shell, comme ont pu le constater les analystes de GSTC lors de leurs investigations.

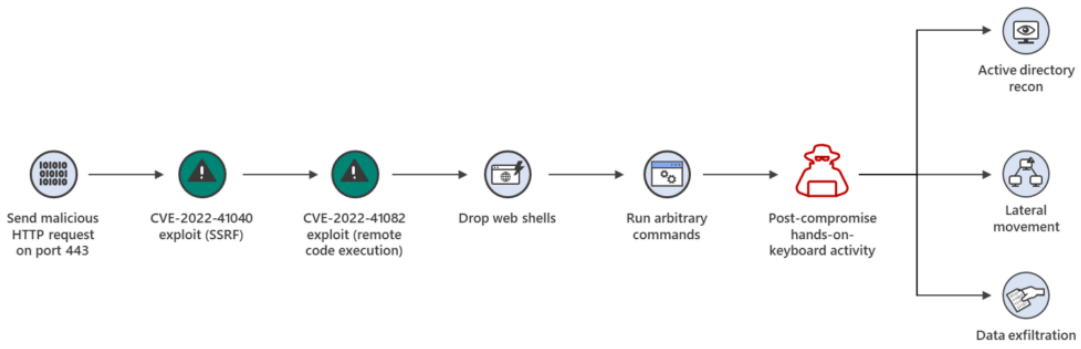

Figure 3. Chaîne d'attaque avec l'exploitation conjointe des CVE-2022-41040 et CVE-2022-41082.

1.2. Atténuation du risque

Microsoft n'a pas encore publié de correctifs pour ces vulnérabilités. Toutefois, l'entreprise américaine, met à disposition un script powershell qui configure des règles de filtrage sur le module *URL Rewrite* du serveur IIS.

Ce dispositif permettra d'interrompre la chaîne d'attaque, empêchant ainsi l'exploitation de la RCE.

Le pattern intégré dans les règles de filtrage **.autodiscover\.json.**\@.**Powershell.** ressemble à celle de la vulnérabilité Proxyshell.

Mise à jour du 04 octobre 2022 : Microsoft recommande de désactiver l'accès à Powershell à distance pour les utilisateurs non administrateurs.
Il conviendra de tester cette configuration pour identifier les éventuels effets de bord.

Pour les serveurs Exchange dotés de Microsoft 365 Defender, Microsoft préconise le paramétrage de l'EDR en mode ***Block mode*** ainsi que l'activation des modules :

- **cloud-delivered** protection,
- **tamper protection**, qui permet de lever une alerte lors de l'arrêt d'un service de sécurité,
- **network protection**,
- **investigation and remediation** en automatique.

1.3. Recherche de compromission

Pour déterminer si la vulnérabilité SSRF a été exploitée sur votre serveur Exchange, exécuter la commande ci-dessous depuis une console powershell.

```
Get-ChildItem -Recurse -Path <Path_IIS_Logs> -Filter "*.log" | Select-String -Pattern
'powershell.*autodiscover\.json.*\@.*200'
```

Par défaut, les journaux d'activités IIS sont localisés à cet emplacement : %SystemDrive%\inetpub\logs\LogFiles

Dans son article du 01 octobre, Microsoft met à disposition pour *Microsoft 365 Defender* deux requêtes pour détecter la présence du webshell Chopper ainsi que des fichiers suspects dans le dossiers du serveur Exchange.

Chopper webshell

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "w3wp.exe"
| where ProcessCommandLine has_any ("&ipconfig&echo", "&quser&echo", "&whoami&echo", "&c:&echo",
"&cd&echo", "&dir&echo", "&echo [E]", "&echo [S]")
```

Fichiers suspects

```
DeviceFileEvents
| where Timestamp >= ago(7d)
| where InitiatingProcessFileName == "w3wp.exe"
| where FolderPath has "FrontEnd\\HttpProxy\\"
| where InitiatingProcessCommandLine contains "MSExchange"
| project FileName,FolderPath,SHA256, InitiatingProcessCommandLine, DeviceId, Timestamp
```

2. Références

- https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers?view=exchange-ps&viewFallbackFrom=exchange-ps%22%20%5Cl%20%22use-the-exchange-management-shell-to-enable-or-disable-remote-powershell-access-for-a-user