CVE 2022-30190

“Follina”

Nicolas GUERROUDJ
Tanguy PAYMAL

08/12/2022

Introduction

La CVE 2022-30190 aussi appelé Follina est un faille zero day qui a été découverte le 30 mai 2022 par Microsoft. Elle permet d'exécuter du code (RCE) sur une machine utilisant une instance de Windows (Serveur ou client) via le logiciel Microsoft Support Diagnostic Tools (MSDT).

La faille est exploitée en local et permet à l'attaquant d'exécuter du code pour ensuite avoir un accès à la machine avec les droits de l'utilisateur piégé. L'attaquant crée un document Microsoft Word avec une payload bien particulière pour exploiter la faille de l'outil MSDT. Pour infecter une machine, l'attaquant peut utiliser des méthodes de phishing ou encore laisser des clés USB au sol. Pour déclencher l'attaque plusieurs moyens sont possibles, l'utilisateur click sur le document word pour l'ouvrir, "single-click", mais il est possible aussi de faire l'attaque en "zero-click" si l'utilisateur utilise des logiciels proposant un aperçu des documents.

L'intégrité, la confidentialité et la disponibilité sont compromises. L'attaquant à le même niveau de contrôle sur la machine que l'utilisateur. Le niveau de complexité de l'attaque est faible et elle ne nécessite pas de droits spécifiques.

Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) dans son bulletin CERTFR-2022-ALE-005 [2], les systèmes suivants sont vulnérables :

- Windows 10 Version 1607 pour systèmes 32 bits
- Windows 10 Version 1607 pour systèmes x64
- Windows 10 Version 1809 pour systèmes 32 bits
- Windows 10 Version 1809 pour systèmes ARM64
- Windows 10 Version 1809 pour systèmes x64
- Windows 10 Version 20H2 pour systèmes 32 bits
- Windows 10 Version 20H2 pour systèmes ARM64
- Windows 10 Version 20H2 pour systèmes x64
- Windows 10 Version 21H1 pour systèmes 32 bits
- Windows 10 Version 21H1 pour systèmes ARM64
- Windows 10 Version 21H1 pour systèmes x64
- Windows 10 Version 21H2 pour systèmes 32 bits
- Windows 10 Version 21H2 pour systèmes ARM64
- Windows 10 Version 21H2 pour systèmes x64
- Windows 10 pour systèmes 32 bits
- Windows 10 pour systèmes x64
- Windows 11 pour systèmes ARM64
- Windows 11 pour systèmes x64
- Windows 7 pour systèmes 32 bits Service Pack 1
- Windows 7 pour systèmes x64 Service Pack 1
- Windows 8.1 pour systèmes 32 bits
- Windows 8.1 pour systèmes x64

- Windows RT 8.1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (Server Core installation)
- Windows Server 2008 pour systèmes 32 bits Service Pack 2
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 (Server Core installation)
- Windows Server 2008 pour systèmes x64 Service Pack 2
- Windows Server 2008 pour systèmes x64 Service Pack 2 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2022
- Windows Server 2022 (Server Core installation)
- Windows Server 2022 Azure Edition Core Hotpatch
- Windows Server, version 20H2 (Server Core Installation)

Démonstration de la vulnérabilité

Pour effectuer la démonstration de la vulnérabilité, merci de bien vouloir suivre les consignes suivantes avec précaution.
Toutefois, si une des étapes ci-dessus ne fonctionne pas, ou en cas de difficultés vous pouvez regarder la vidéo de la démonstration réalisée par nos soins en cliquant **ici**.

0 - Prérequis

- Vagrant
- VirtualBox

1 - Installation de la machine virtuelle

La première étape va être de mettre en place le script vagrant “VagrantFile” correspondant à la machine virtuelle de la démonstration.
Pour ce faire, vous pouvez cloner le repository du rendu et vous servir du VagrantFile déjà fourni. Ou alors copier le contenu du VagrantFile ci-dessous:

```
Vagrant.configure("2") do |config|

  config.vm.box = "tan9uy/follina-cve-2022-30190"
  config.vm.box_version = "3.0.0"

  # Additional parameters to communicate with Windows
  config.vm.boot_timeout = 600
  config.vm.communicator = "winrm"
  config.winrm.port = 55985

  config.vm.provider "virtualbox" do |v|
    v.name = "Follina"
    v.gui = true
    v.memory = 2048
    v.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
    v.customize ["modifyvm", :id, "--clipboard", "bidirectional"]
    v.cpus = 2
  end
end
```

Une fois le VagrantFile créé, il suffit d’exécuter la commande suivante dans le même répertoire que le fichier pour démarrer la machine virtuelle:

```
vagrant up
```

Si la machine ne se lance pas automatiquement via la commande ci-dessus. Essayez de la démarrer depuis VirtualBox.

Attention: Cette opération peut prendre beaucoup de temps. En effet, l'image de la machine virtuelle est très lourde (22Go). Si vous effectuez cette opération sur les machines de l'Ensimag, veillez à vous situer dans votre répertoire "scratch":

```
mkdir -p /scratch/$(whoami) && cd /scratch/$(whoami)
export VAGRANT_HOME=/scratch/$(whoami)
vagrant up
```

2 - Exécution du script compromis

Une fois la machine virtuelle installée et démarrée vous pouvez ouvrir la session de l'utilisateur "vagrant" en utilisant le mot de passe "vagrant".
Vous trouverez alors sur le bureau un script nommé "install.bat" que vous pouvez exécuter en tant qu'administrateur.

Attention: Ce script génère un fichier Word nommé "clickme" et démarre un serveur exposant une payload spécifique en arrière-plan. Ce script est uniquement nécessaire dans le cadre de la démonstration. Ainsi, en temps "normal", il n'est pas nécessaire, vous pouvez alors simplement imaginer recevoir le fichier "clickme" par mail.

3 - Ouvrir le document Word.

Une fois le script d'installation exécuté/avoir reçu par "mail" le document word "clickme". Vous décidez de l'ouvrir en double cliquant dessus.

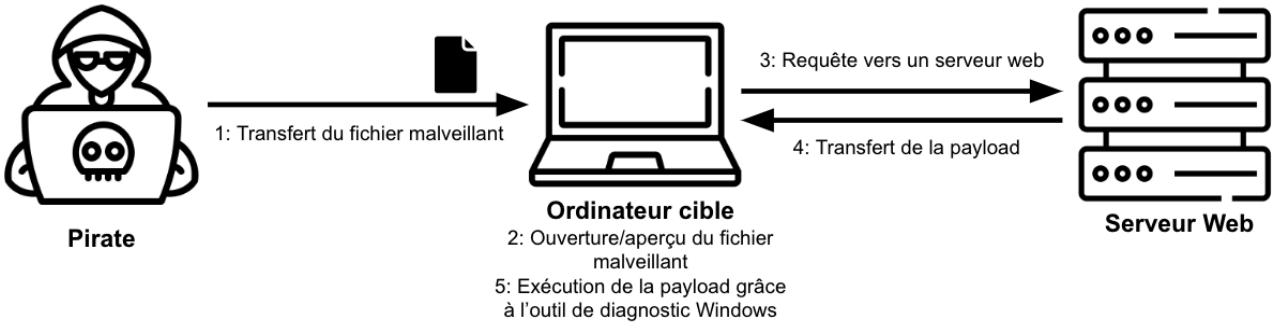
Attention: Il ne faut pas ouvrir le fichier Word en "Safe mode".

4 - Enjoy

Félicitations vous avez été "piraté" !

Vous pouvez découvrir comment vous vous êtes fait pirater dans la section suivante.

Explication de vulnérabilité



1 - Transfert du fichier malveillant

La première étape pour l'exploitation de cette vulnérabilité peut paraître simple mais est sans doute la plus compliquée. En effet, cette étape consiste à infecter l'ordinateur cible avec le fichier malveillant.

Pour cela, il existe plusieurs méthodes. La première consiste à envoyer le fichier malveillant par mail à l'utilisateur cible. Cette méthode est très répandue et peut être très efficace. En effet, il est facile de se faire passer pour une personne de confiance et d'envoyer un mail contenant un fichier malveillant.

La seconde méthode consiste à créer un lien malveillant sur un site internet. L'utilisateur cible peut alors cliquer sur ce lien et être redirigé vers le fichier malveillant.

La dernière méthode consiste à laisser des clés USB dans des lieux de visite régulière de la cible. Celle-ci pourra alors être tenté de garder cette clé USB perdue et d'ouvrir le contenu qu'elle contient. Restez donc prudents aux périphériques que vous branchez à votre ordinateur.

Le fichier malveillant prend la forme d'un document Word, qui se présente sous la forme d'une sorte d'archives contenant d'autres fichiers nécessaires au bon fonctionnement de l'application.

2 - Ouverture/aperçu du fichier malveillant

Cette étape peut nécessiter ou non l'action de l'utilisateur. Le but de cette étape est que l'utilisateur infecté clique et ouvre le document word. Mais dans certains cas, comme avec des logiciels de prévisualisation des documents, l'utilisateur n'aurait même pas besoin de cliquer sur le document pour se faire infecter.

3 - Requête vers un serveur web

Par défaut, dans l'archive qui constitue le document word, on trouve le document document.xml.ref. Dans ce document l'attaquant va changer un lien d'une ressource externe pour le faire pointer vers un serveur malicieux.

4 - Transfert de la payload

Le changement dans le document documents.xml.ref va permettre, quand l'utilisateur ouvrira le document de chercher une payload qui sera accessible via l'URL défini dans le document. Pour l'utilisateur cette étape se passe en arrière plan, il n'a aucune idée qu'il a exécuté un document malicieux.

5 - Exécution de la payload

Enfin la dernière étape est l'exécution du code malveillant sur l'ordinateur en utilisant la faille de l'outil MSDT. La payload utilisée pour exploiter la faille est la suivante :

```
ms-msdt:/id PCWDiagnostic /skip force /param \\"IT_RebrowseForFile=?
IT_LaunchMethod=ContextMenu
IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]
'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBas
e64String('+[char]34+'{base64_payload}'+[char]34+'))'))))i/../../../../../../../
../../../../../../../Windows/System32/mpsigstub.exe\\""; //
```

Dans cette payload, on peut ensuite exécuter directement des commandes powershell encoder en base 64. Ces commandes peuvent permettre d'exécuter n'importe quelle code en utilisant les droits de l'outil MSDT qui sont en générale le même que l'utilisateur de la machine. Cela veut dire que si l'utilisateur est administrateur sur sa machine, l'attaquant peut aussi faire des commandes en tant qu'administrateur.

Gestion de la faille

Gestion lors de l’attaque

En se plaçant dans la peau d’un administrateur des systèmes d'information, la première chose à faire selon nous est de mettre à jour l’ensemble des appareils (serveur, client) avec le correctif proposé par Microsoft. Cela va permettre de limiter le nombre d’appareils infectés.

Etant donné que c’était une faille zero day et que le fix n’est pas sortie directement, il faut pouvoir réagir plus tôt pour limiter l’impact. Dans ce cas, nous conseillons de bien activer Windows Defender qui met à jour sa base de détection régulièrement à jour via internet. Le chargement de la ressource externe malicieuse sera détecté avant l'exécution de la payload.

Une autre possibilité, est de supprimer la clé de registre HKEY_CLASSES_ROOT\ms-msd et ainsi même si la payload est présente sur l’appareil, l’exécution de la faille MSDT ne fonctionnera pas.

Une fois que les appareils sont protégés via ces différentes actions, la seconde étape est de trouver les appareils qui ont été infectés et où l’outil MSDT à exécuter la payload. Pour cela l’outil MSDT utilise plusieurs dossiers de diagnostic (%LOCALAPPDATA%\Diagnostics, %LOCALAPPDATA%\ElevatedDiagnostics). Par la suite, une étude plus approfondie peut être réalisée pour comprendre quelle payload à été exécuté et prendre des mesures adaptées.

La politique des systèmes d’information

Il existe plusieurs politiques de systèmes d'information qui peuvent être mis en place par une entreprise pour prévenir des différentes failles de sécurité:

1. Mettre à jour régulièrement les logiciels et les systèmes d'exploitation utilisés par l'entreprise pour s'assurer qu'ils sont protégés contre les dernières failles de sécurité connues.

2. Appliquer les derniers correctifs de sécurité dès qu'ils sont disponibles.

3. Utiliser un pare-feu strict pour protéger les réseaux de l'entreprise contre les attaques extérieures.

4. Former et sensibiliser les employés à la sécurité informatique pour qu'ils sachent comment identifier et éviter les tentatives d'intrusion (phishing, lien de téléchargement douteux, clé usb perdue)

5. Utiliser des logiciels de détection et de prévention des intrusions pour détecter les tentatives d'intrusion et les bloquer avant qu'elles ne puissent causer des dommages.

6. Imposer des restrictions d'accès aux données sensibles et forcer les employés à utiliser des mots de passe forts pour protéger les comptes d'utilisateurs.

7. Sauvegarder régulièrement les données de l'entreprise pour pouvoir les restaurer en cas de perte ou de corruption des données.

D’une manière générale, il est important de se tenir informé un maximum des nouvelles vulnérabilités et failles connues afin de pouvoir prendre les mesures nécessaires pour protéger les systèmes et les données de l'entreprise. Pour cela, il est recommandé de suivre les dernières actualités en matière de sécurité informatique et de s'abonner à des bulletins d'alerte émis par les organismes de sécurité, les fabricants de logiciels et les fournisseurs de services en ligne.

Il est également important de participer à des événements et des conférences sur la sécurité informatique pour rester informé des dernières tendances et développements en matière de sécurité. De plus, il est utile de s'engager dans des programmes de certification en sécurité informatique pour améliorer ses connaissances et ses compétences en la matière.

Ainsi, en mettant en place ces politiques de systèmes d'informations, une entreprise peut réduire significativement les risques de faille de sécurité et protéger ses données et ses systèmes contre les attaques informatiques.

Bibliographie

- [1] Maxime ALAY-EDDINE, article sur le site cyberwatch.fr, 31 mai 2022 https://cyberwatch.fr/cve/comment-detecter-et-traiter-la-cve-2022-30190-follina/
- [2] Bulletin d'alerte de l'ANSSI, 31 mai 2022 https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-005/
- [3] Publication de Microsoft, 30 mai 2022, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
- [4] Dawid Farbaniec, 25 juin 2022, https://ethical.blue/textz/n/32
- [5] Detect the Follina MSDT Vulnerability (CVE-2022-30190) with Qualys Multi-Vector EDR & Context XDR, 14 juin 2022, https://blog.qualys.com/product-tech/2022/06/14/detect-the-follina-msdt-vulnerability-cve-2022-30190-with-qualys-multi-vector-edr-context-xdr
- [6] Let's play with a ZERO-DAY vulnerability "follina", 1 juin 2022, https://www.youtube.com/watch?v=3ytqP1QvhUc