Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 31 mai 2022
N° CERTFR-2022-ALE-005

Affaire suivie par: CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet: [MàJ] Vulnérabilité dans Microsoft Windows

Gestion du document

Référence	CERTFR-2022-ALE-005
Titre	[MàJ] Vulnérabilité dans Microsoft Windows
Date de la première version	31 mai 2022
Date de la dernière version	01 juin 2022
Source(s)	Bulletin de sécurité Microsoft CVE-2022-30190 du 30 mai 2022 Billet de blogue Microsoft du 30 mai 2022
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Risque(s)

- Exécution de code arbitraire à distance

Systèmes affectés

- 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)

Résumé

[Mise à jour du 01 juin 2022] Ajout d'une règle Sigma à la portée plus large.

Le 27 mai 2022, un chercheur a identifié un document Word piégé sur la plate-forme *Virus Total* . Lorsque ce document est ouvert, l'un des objets *OLE (Object Linking and Embedding)* présent dans celui-ci télécharge du contenu situé sur un serveur externe contrôlé par l'attaquant. Ce contenu exploite une vulnérabilité permettant d'exécuter du code malveillant *via* le binaire légitime *Microsoft Support Diagnostic Tool (MSDT)*, *msdt.exe*, sous la forme d'un script *Powershell* encodé en base 64. Il convient de noter que cette attaque fonctionne y compris lorsque les macros sont désactivées dans le document Office.

Le 30 mai 2022, Microsoft a publié un avis de sécurité (cf. section Documentation) dans lequel l'éditeur confirme la vulnérabilité, qui porte l'identifiant CVE-2022-30190, ainsi que les

versions vulnérables du système d'exploitation Windows.

Dans un billet de blogue du même jour (cf. section Documentation), Microsoft indique que si le fichier est ouvert par une application Office, le mode *Protected View* ou *Application Guard for Office* est enclenché et empêche la charge utile de s'exécuter.

Toutefois, plusieurs chercheurs affirment que cette vulnérabilité peut être exploitée à l'aide d'un document au format RTF. Dans ce cas, la charge utile peut ainsi être récupérée et exécutée lorsque le document est prévisualisé (par exemple dans *Windows Explorer*) et donc sans qu'il ne soit ouvert par l'utilisateur.

Cette vulnérabilité semble être utilisée dans des attaques ciblées et Microsoft n'a pas annoncé de date de publication d'un correctif.

Le CERT-FR propose la règle Sigma suivante, encore expérimentale, pour tenter de détecter l'exploitation de la vulnérabilité CVE-2022-30190 (ne pas oublier de renommer le .txt en .yml) :

Télécharger la règle Sigma CVE-2022-30190

[Mise à jour du 01 juin 2022]

Plusieurs chercheurs indiquent que d'autres vecteurs d'attaque peuvent être utilisés pour appeler abusivement l'exécutable *msdt.exe*. Ceux-ci citent notamment l'utilisation de la commande *wget* disponible avec *Powershell*. Le CERT-FR propose donc une nouvelle règle Sigma qui cherche aussi à détecter l'utilisation de *msdt.exe* en dehors du contexte *Microsoft Office* (ne pas oublier de renommer le .txt en .yml).

Télécharger la règle Sigma CVE-2022-30190_2

Contournement provisoire

L'exécution du binaire *msdt.exe* par un document Office n'est pas une pratique courante, le CERT-FR recommande donc d'appliquer le contournement documenté par l'éditeur dans son billet de blogue du 30 mai 2022.

Microsoft propose de désactiver le protocole URL de MSDT en utilisant la commande suivante, à lancer dans une invite de commandes avec les droits administrateur, après avoir sauvegardé le registre :

```
reg delete HKEY_CLASSES_ROOT\ms-msdt /f
```

La modification du registre est une opération délicate qui doit être menée avec prudence. Il est notamment recommandé d'effectuer des tests autant que possible.

Documentation

- Bulletin de sécurité Microsoft CVE-2022-30190 du 30 mai 2022
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
- Billet de blogue Microsoft du 30 mai 2022
  https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
- Référence CVE CVE-2022-30190
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190

Gestion détaillée du document

le 31 mai 2022
Version initiale

le 01 juin 2022
Ajout d'une deuxième règle Sigma.

le 01 juin 2022
Correction d'un problème d'indentation dans la règle Sigma CVE-2022-30190_2.