NEWSCAST CYBER THREAT INTELLIGENCE

MICROSOFT CVE-2022-30190

CERT ADVENS

15/06/2022 / TLP-WHITE

SOMMAIRE

01 MICROSOFT CVE-2022-30190

01.1 RESUME

Signalée le 30 mai 2022 par l'entreprise Microsoft, la CVE-2022-30190 est une vulnérabilité activement exploitée qui affecte plusieurs systèmes d'exploitation et serveurs Windows. Cette CVE est aussi connue par son surnom « **msdt follina** ».

La vulnérabilité concerne l'outil de diagnostic du support Microsoft (MSDT), il s'agit d'un outil légitime qui collecte des informations du système pour les envoyer au service *Support Microsoft*. Ce service réalise une analyse des informations reçues afin de proposer une résolution d'un problème auquel fait face l'utilisateur.

Un document Word malveillant peut être réalisé par un attaquant qui dissimule dans celui-ci une charge utile. Lorsqu'un utilisateur ouvre le document après y avoir été incité, la charge utile s'active et lance un appel MSDT via le protocole URL. L'exploitation d'un défaut dans cette procédure permet à l'attaquant d'exécuter du code arbitraire sur le système de l'utilisateur sans avoir recours aux macros.

Le code est exécuté avec le même niveau de privilège que l'application Microsoft Office lors de l'ouverture du document forgée. L'exploitation de cette vulnérabilité peut permettre à l'attaquant d'installer de nouveaux programmes, de porter atteinte à la confidentialité et à l'intégrité des données, et de créer de nouveaux comptes utilisateurs.

Point important : la version « **0-click RTF version** ».

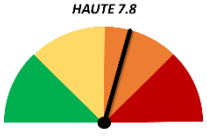
Selon l'expertise ayant publié l'exploit, une version encore plus redoutable existe. Il est possible d'ajouter trois lignes de codes malveillantes dans le document Word et d'enregistrer celui-ci en document rtf. **Cet enregistrement est considéré comme plus redoutable, car il permet l'activation de la charge utile sans ouvrir le document, un simple aperçu du document est suffisant pour réaliser l'exécution de code arbitraire.**

La CVE-2022-30190 aurait récemment été exploitée lors de plusieurs cyberattaques à l'encontre du gouvernement ukrainien, à l'encontre de plusieurs agences du gouvernement des États-Unis et Européens, et lors d'une campagne de déploiement du logiciel malveillant Qbot. Selon Proofpoint, l'APT chinois TA413 exploiterait aussi cette vulnérabilité depuis début juin à l'encontre de la Diaspora tibétaine.

01.2 INFORMATIONS

01.2.1 | RISQUES

- Exécution de code arbitraire à distance
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données



- Élévation de privilèges

01.2.2 | CRITICITE

- **La faille est activement exploitée**
- **Vecteur d'attaque : Local** *(Microsoft précise que l'attaquant est distant, mais que la réalisation de l'offensive est locale)*
- **Complexité d'attaque : Faible**
- **Privilèges requis : Aucun**
- **Interaction de l'utilisateur : Oui**
- **Portée : Inchangée**
- **Impact sur la confidentialité : Haute**
- **Impact sur l'intégrité : Haute**
- **Impact sur la disponibilité : Haute**

01.2.3 | COMPOSANTS VULNERABLES.

Ci-dessous, la liste des produits concernés :

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2008 R2 X64
- Microsoft Windows Server 2012
- Microsoft Windows RT
- Microsoft Windows 8.1 x32
- Microsoft Windows 8.1 x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows RT 8.1
- Microsoft Windows 10 x32
- Microsoft Windows 10 x64
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows 10 1809 x64-based Systems
- Microsoft Windows 10 1809 32-bit Systems
- Microsoft Windows 10 1809 ARM64-based Systems

- Microsoft Windows 10 1607 32-bit Systems
- Microsoft Windows 10 1607 x64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 ARM64-based Systems
- Microsoft Windows 10 20H2 x64-based Systems
- Microsoft Windows Server (Server Core installation) 2019
- Microsoft Windows Server (Server Core installation) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server (Server Core installation) 2012
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 R2
- Microsoft Windows Server X64-based systems 2008 R2 SP1
- Microsoft Windows Server 32-bit systems (Server Core installation) 2008 SP2
- Microsoft Windows Server 32-bit systems 2008 SP2
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 R2 SP1
- Microsoft Windows 10 21H1 32-bit Systems
- Microsoft Windows 10 21H1 ARM64-based Systems
- Microsoft Windows 10 21H1 x64-based Systems
- Microsoft Windows Server 2022
- Microsoft Windows Server (Server Core installation) 2022
- Microsoft Windows Server X64-based systems 2008 SP2
- Microsoft Windows 11 x64
- Microsoft Windows 11 ARM64
- Microsoft Windows 10 21H2 32-bit Systems
- Microsoft Windows 10 21H2 ARM64-based Systems
- Microsoft Windows 10 21H2 x64-based Systems
- Microsoft Windows Server 2022 Azure Edition Core Hotpatch

01.3 RECOMMANDATIONS

- Une mise à jour de Microsoft existe, le Patch Tuesday juin 2022, et permet d'apporter le correctif nécessaire.

- Des informations complémentaires sont disponibles ici.
- Des informations complémentaires concernant Windows Defender sont disponibles ici.

Les mises à jour de sécurité cumulative, datées du 14 juin 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 8.1, Windows server 2012 R2: KB5014738 KB5014746
- Windows server 2012: KB5014747 KB5014741
- Windows 7, Windows server 2008 R2: KB5014748 KB5014742
- Windows server 2016: KB5014702
- Windows 10 : KB5014710 KB5014699
- Windows 11: KB5014697
- Windows Server 2019: KB5014692
- Windows Server 2022: KB5014678

- Une solution de contournement existe, celle-ci est décrite ci-dessous.

Désactiver le protocole URL pour MSDT permet d'éviter qu'un attaquant exploite la vulnérabilité pour réaliser son offensive. Une demande de support est toujours possible via l'application Recevoir de l'aide, ou par d'autres moyens fournis par le système d'exploitation.

Désactiver le protocole URL pour MSDT :

1- Utiliser l'invite de commande en tant qu'administrateur.

2- Sauvegarder la clé registre avec la commande : *reg export HKEY_CLASSES_ROOT\ms-msdt filename*

3- Exécuter la commande *reg delete HKEY_CLASSES_ROOT\ms-msdt /f*

Réactiver le protocole URL pour MSDT :

1- Utiliser l'invite de commande en tant qu'administrateur.

2- Exécuter la commande (pour utiliser la sauvegarde de la clé, registre) : *reg import filename*

01.4 PROOF OF CONCEPT

Des exploits (POC) sont disponibles en sources ouvertes.

02 REFERENCES

https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

https://exchange.xforce.ibmcloud.com/vulnerabilities/227557

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190

https://www.bleepingcomputer.com/news/security/qbot-malware-now-uses-windows-msdt-zero-day-in-phishing-attacks/

https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2022-patch-tuesday-fixes-1-zero-day-55-flaws/

advens
CYBERSECURITY

advens.fr

Lille +33 3 20 68 41 81
Paris +33 1 84 16 30 25
Lyon +33 4 28 29 08 29
Bordeaux +33 5 35 54 82 84