Security for the greater good

Renseignement sur les menaces

Bulletin Patch Tuesday Juillet 2022

CERT ADVENS

13/07/2022 - TLP WHITE

Sommaire

1 Patch Tuesday Microsoft

Le 13 juillet 2022, Microsoft a publié son Patch Tuesday qui corrige 84 vulnérabilités, dont quatre considérées comme critiques et une zero-day.

Cette dernière, référencée CVE-2022-22047, impacte le sous-système d'exécution client/serveur (CSRSS). Selon Microsoft, elle serait activement exploitée.

Ce bulletin aborde les vulnérabilités ci-dessous :

CSRSS

CVE-2022-22047

Graphique

CVE-2022-30221

RPC

CVE-2022-22038

NFS

CVE-2022-22029

CVE-2022-22039

Print Spooler

CVE-2022-22022

CVE-2022-22041

CVE-2022-30206

CVE-2022-30226

Azure Site Recovery

CVE-2022-33674

2 CSRSS CVE-2022-22047

2.1 Résumé

Découverte par les deux équipes Microsoft, Threat Intelligence Center (MSTIC) et Security Response Center (MSRC), la CVE-2022-2247 est une vulnérabilité critique et activement exploitée. Elle affecte plusieurs serveurs et systèmes d'exploitation Windows.

Les experts ont identifié un défaut dans le sous-système d'exécution client/serveur (CSRSS). La limite de la taille de l'information traitée est configurée de manière incorrecte. Il est ainsi possible, pour un attaquant détenant un accès au système en tant que simple utilisateur, d'exécuter du code arbitraire avec les privilèges les plus élevés.

Aujourd'hui, malgré la mise en évidence d'une exploitation active de cette vulnérabilité par l'éditeur, aucune preuve de concept n'existe en sources ouvertes.

Comme l'indique Dustin Child de *Zero Day Initiative*, ce type de vulnérabilité est exploité à la suite d'une compromission du système.

2.2 Information

2.2.1 Risque

- Exécution de code arbitraire
- Élévation de privilèges

2.2.2 Criticité

- La faille est activement exploitée
- Vecteur d'attaque : Local
- Complexité d'attaque : Faible
- Privilèges requis : Faible
- Interaction de l'utilisateur : Non
- Portée : Inchangée
- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

2.2.3 Composants vulnérables

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2012
- 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 2008 R2 SP1
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 SP2
- 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

2.3 Recommandation

- Une mise à jour de Microsoft existe. Le Patch Tuesday juillet 2022 apporte les correctifs nécessaires.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité du 12 juillet 2022, pour les produits concernés sont les suivantes.

- Windows 8.1, Windows serveur 2012 : 5015877, 5015874, 5015863, 5015875, 5015863
- Windows serveur 2008, Windows 7 : 5015861, 5015862, 5015866, 5015870
- Windows serveur 2016, Windows 10 : 5015808, 5015832, 5015807
- Windows 11 : 5015814
- Windows serveur 20H2, Windows 10 Version 21H1 : 5015807
- Windows serveur 2022 : 5015827
- Windows serveur 2019, Windows 10 Version 1809 : 5015811

2.4 Proof of Concept

- Aucun exploit n'est disponible pour le moment en sources ouvertes.

3 Graphique CVE-2022-30221

3.1 Résumé

Cette vulnérabilité a été découverte à la suite d'un travail collaboratif entre plusieurs experts et l'équipe de cybersécurité Thalium. Considérée comme critique, elle impacte le composant graphique du système d'exploitation Windows.

Les experts ont mis en exergue que le composant graphique de Windows réalise un contrôle insuffisant des données entrées par l'utilisateur. Ainsi, du code malveillant peut être injecté dans le composant graphique pour qu'il soit exécuté. Son exploitation peut être réalisée par un attaquant distant et non authentifié.

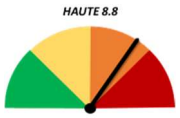
Cette vulnérabilité peut être exploitée de manières différentes :

- Selon Microsoft, Cybersecurity-Help et Qualys, un attaquant peut inciter un utilisateur à établir une connexion avec un serveur RDP, maîtrisé par l'attaquant. Ce dernier l'utilise pour exécuter du code arbitraire sur le système de l'utilisateur. **Point particulier : ce scénario d'attaque ne peut être accompli que sur le système Windows 7 SP1 ou Windows Server 2008 R2 SP1 si RDP 8.0 ou 8.1 est installé.**
- Selon IBM-XForce, un attaquant peut inciter un utilisateur à ouvrir un fichier spécifiquement forgé. A son ouverture, une charge utile s'active et permet l'exécution de code arbitraire sur le système de l'utilisateur.

3.2 Information

3.2.1 Risque

- Exécution de code arbitraire à distance



3.2.2 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Réseau
- 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

3.2.3 Composants vulnérables

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- 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) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server X64-based systems 2008 R2 SP1
- 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 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

3.3 Recommandation

- Une mise à jour de Microsoft existe. Le Patch Tuesday juillet 2022 apporte les correctifs nécessaires.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité du 12 juillet 2022, pour les produits concernés sont les suivantes.

- Windows 8.1, Windows serveur 2012 : 5015877, 5015874
- Windows serveur 2008, Windows 7 : 5015861, 5015862
- Windows serveur 2016, Windows 10 : 5015808, 5015832
- Windows 11 : 5015814
- Windows serveur 20H2, Windows 10 Version 21H1 : 5015807
- Windows serveur 2019, Windows 10 Version 1809 : 5015811

3.4 Proof of Concept

- Aucun exploit n'est disponible pour le moment en sources ouvertes.

4 RPC CVE-2022-22038

4.1 Résumé

La société chinoise de développement de logiciel de cybersécurité, Cyber KunLun, et Yuki Chen (spécialiste de la chasse au bug) ont signalé la CVE-2022-22038 : il s'agit d'une vulnérabilité critique localisée dans la technologie d'appel de procédure distant RPC (Remote Procedure Call Runtime, RPCR).

Il a été découvert que l'application d'appel de procédure distant réalise un contrôle limité des données traitées lors de son exécution. Une requête peut être spécifiquement forgée de manière à contenir une charge utile. Lors du traitement de la requête forgée, la charge utile se déclenche et du code arbitraire est alors exécuté sur le système sans que le contrôle intégré à l'appel de procédure distant ne le détecte.

L'exploitation de cette vulnérabilité est réalisée à distance et aucune authentification n'est nécessaire.

Point important : Microsoft précise que le niveau de complexité de l'attaque est élevé. En effet, l'attaquant doit investir énormément de temps pour mener des exploitations répétées en envoyant des requêtes de manière constante ou par intermittence.

4.2 Information

4.2.1 Risque

- Exécution de code arbitraire à distance

4.2.2 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Réseau
- Complexité d'attaque : Haute
- Privilèges requis : Aucun
- Interaction de l'utilisateur : Non
- Portée : Inchangée
- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

4.2.3 Composants vulnérables

- Microsoft Windows Server 2012
- 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 for ARM64-based Systems
- Microsoft Windows 10 20H2 for 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 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 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

4.3 Recommandation

- Une mise à jour de Microsoft existe. Le Patch Tuesday juillet 2022 apporte les correctifs nécessaires.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité du 12 juillet 2022, pour les produits concernés sont les suivantes.

- Windows 8.1, Windows serveur 2012 : 5015877, 5015874, 5015863, 5015875
- Windows serveur 2016, Windows 10 : 5015808
- Windows 11 : 5015814
- Windows serveur 2022 : 5015827
- Windows serveur 20H2, Windows 10 Version 21H1 : 5015807
- Windows serveur 2019, Windows 10 Version 1809 : 5015811

4.4 Proof of Concept

- Aucun exploit n'est disponible pour le moment en sources ouvertes.

5 NFS CVE-2022-22029 / 22039

5.1 Résumé

Cyber KunLun et Yuki Chen ont aussi signalé les deux CVE-2022-22029 / 22039. Deux vulnérabilités importantes localisées dans le système de fichier réseau (Network File System, NFS).

Le système de fichier réseau NFS aurait un défaut de contrôle des données traitées. Une requête spécifiquement forgée, contenant une charge utile, peut être utilisée pour exécuter du code arbitraire sur le système. La charge utile est déclenchée lors du traitement de la requête sans que le contrôle des données signale la malveillance.

- Pour la CVE-2022-22029, l'attaque est réalisée à distance et aucune authentification n'est nécessaire. Microsoft précise que le niveau de complexité de l'attaque est élevé, au vu du temps engagé par l'attaquant pour la réaliser. En effet, celui-ci doit mener des tentatives répétées en envoyant des requêtes de manière constante ou par intermittence.

- Pour la CVE-2022-22039, l'attaque est elle aussi réalisée à distance, cependant une authentification en tant que simple utilisateur est nécessaire. De plus, Microsoft précise que l'attaquant doit au préalable réussir à gagner une condition de concurrence (la CVE-2022-22039 est de type « race condition »).

5.2 Information

5.2.1 Risque CVE-2022-22029

- Exécution de code arbitraire à distance

5.2.2 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Réseau
- Complexité d'attaque : Haute
- Privilèges requis : Aucun
- Interaction de l'utilisateur : Non
- Portée : Inchangée

- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

5.2.3 Risque CVE-2022-22039

- Exécution de code arbitraire à distance

5.2.4 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Réseau
- Complexité d'attaque : Haute
- Privilèges requis : Faible
- Interaction de l'utilisateur : Non
- Portée : Inchangée
- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

5.2.5 Composants vulnérables

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- 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 2008 R2 SP1

- Microsoft Windows Server X64-based systems (Server Core installation) 2008 SP2
- 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 Server 2022
- Microsoft Windows Server (Server Core installation) 2022
- Microsoft Windows Server X64-based systems 2008 SP2

5.3 Recommandation

- Une mise à jour de Microsoft existe. Le Patch Tuesday juillet 2022 apporte les correctifs nécessaires.
- Des informations supplémentaires sont disponibles ici et ici.

Les mises à jour de sécurité du 12 juillet 2022, pour les produits concernés sont les suivantes.

- Windows 8.1, Windows serveur 2012 : 5015877, 5015874, 5015863, 5015875
- Windows serveur 2008, Windows 7 : 5015861, 5015862, 5015866, 5015870
- Windows serveur 2016, Windows 10 : 5015808
- Windows serveur 2022 : 5015827
- Windows serveur 20H2, Windows 10 Version 21H1 : 5015807
- Windows serveur 2019, Windows 10 Version 1809 : 5015811

5.4 Proof of Concept

- Aucun exploit n'est disponible pour le moment en sources ouvertes.

6 Print Spooler CVE-2022-22022 / 22041 / 30206 / 30226

6.1 Résumé

Plusieurs expertises, notamment Theori et Sangfor, ont étudié quatre vulnérabilités concernant le spooler d'impression du système d'exploitation Windows. Ces quatre vulnérabilités sont les CVE-2022-22022 / 22041 / 30206 et 30226.

Selon Cybersecurity-Help, il a été signalé une sécurité appliquée de manière incorrecte : le spooler d'impression ne dispose pas des restrictions de sécurité adéquates.

- Pour la CVE-2022-22022 / 30226 : Microsoft précise que l'exploitation permet uniquement de porter un impact en supprimant des fichiers sur le système, mais ne permet pas de modifier ou de voir les fichiers. Cependant, IBM X-Force ajoute le risque d'élévation de privilèges et indique que l'exploitation permet une exécution de code arbitraire avec les privilèges les plus élevés.
- Pour la CVE-2022-22041 / 30206 : Microsoft souligne que l'exploitation permet uniquement une élévation de privilèges. De son côté, IBM X-Force indique une exécution de code arbitraire avec les privilèges les plus élevés.

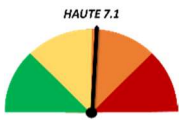
Une solution de contournement existe et celle-ci est valable pour les quatre vulnérabilités : elle est détaillée dans la partie recommandation.

En juillet 2021, Microsoft a publié le correctif pour la célèbre vulnérabilité CVE-2021-34527 (surnommée « Print Nightmare »). Son exploitation permettait à un attaquant d'injecter à distance des librairies malveillantes afin d'exécuter du code arbitraire. Selon Kaspersky, des attaques de type rançongiciels ont été réalisées à l'encontre d'organisations n'ayant pas appliqué le correctif. A ce sujet, Evgeny Lopatin, expert en sécurité chez Kaspersky, précisait dans un article publié sur mtom-mag en juillet 2021 : « Cette faille (CVE-2021-34527) est en effet très sérieuse, car elle permet aux cybercriminels d'accéder à d'autres ordinateurs au sein du réseau d'une organisation. Comme l'exploit est publiquement accessible, de nombreux fraudeurs en tireront parti. **Par conséquent, nous invitons tous les utilisateurs à appliquer les dernières mises à jour de sécurité pour Windows** ».

6.2 Information

6.2.1 Risque CVE-2022-22022

- Porter atteinte à l'intégrité des données
- Exécution de code arbitraire
- Élévation de privilèges (selon IBM X-Force)

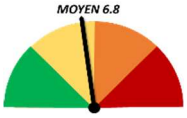


6.2.2 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Local
- Complexité d'attaque : Faible
- Privilèges requis : Faible
- Interaction de l'utilisateur : Non
- Portée : Inchangée
- Impact sur la confidentialité : Aucun
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

6.2.3 Risque CVE-2022-22041

- Exécution de code arbitraire à distance (selon IBM X-Force)
- Élévation de privilèges



6.2.4 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Réseau
- Complexité d'attaque : Faible
- Privilèges requis : Haute
- Interaction de l'utilisateur : Oui
- Portée : Inchangée
- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

6.2.5 Risque CVE-2022-30206

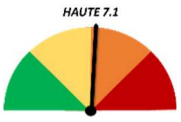
- Exécution de code arbitraire à distance (selon IBM X-Force)
- Élévation de privilèges

6.2.6 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Réseau
- Complexité d'attaque : Faible
- Privilèges requis : Haute
- Interaction de l'utilisateur : Oui
- Portée : Inchangée
- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

6.2.7 Risque CVE-2022-30226

- Porter atteinte à l'intégrité des données
- Exécution de code arbitraire
- Élévation de privilèges (selon IBM X-Force)



6.2.8 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Local
- Complexité d'attaque : Faible
- Privilèges requis : Faible
- Interaction de l'utilisateur : Non
- Portée : Inchangée
- Impact sur la confidentialité : Aucun
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Haute

6.2.9 Composants vulnérables CVE-2022-22022

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2012
- 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 2008 R2 SP1
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 SP2
- 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

6.2.1 Composants vulnérables CVE-2022-22041

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2012
- 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 10 21H1 32-bit Systems
- Microsoft Windows 10 21H1 ARM64-based Systems
- Microsoft Windows 10 21H1 or x64-based Systems
- Microsoft Windows Server 2022
- Microsoft Windows Server (Server Core installation) 2022
- 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

6.2.2 Composants vulnérables CVE-2022-30206

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2012
- 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) 1909
- 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 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 for 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

6.2.3 Composants vulnérables CVE-2022-30226

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2012
- 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 2008 R2 SP1
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 SP2
- 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

6.3 Recommandation

- Une mise à jour de Microsoft existe. Le Patch Tuesday juillet 2022 apporte les correctifs nécessaires.
- Des informations supplémentaires sont disponibles ici, ici, ici et ici.
- Une solution de contournement existe, celle-ci est valable pour les quatre vulnérabilités :

Pour déterminer si le service spooler d'impression est en cours d'exécution

Il faut utiliser la commande la commande PowerShell suivante :

Get-Service – Name Spooler

Si le spooler d'impression est en cours d'exécution, il faut suivre les étapes suivantes :

Arrêter ou désactiver le service spooler d'impression

Si l'arrêt ou la désactivation du service est approprié pour votre environnement de travail, utilisez la commande PowerShell :

Stop-Service – Name Spooler – Force

Set-Service – Name Spooler –Startuptype Disabled

Cette solution de contournement (arrêt et désactivation) empêche l'impression locale et distante.

Les mises à jour de sécurité cumulative, datées du 12 juillet 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 8.1, Windows serveur 2012 : 5015877, 5015874, 5015863, 5015875,
- Windows serveur 2008, Windows 7 : 5015861, 5015862, 5015866, 5015870
- Windows serveur 2016, Windows 10 : 5015808, 5015832
- Windows serveur 20H2, Windows 10 Version 21H1 : 5015807
- Windows serveur 2019, Windows 10 Version 1809 : 5015811
- Windows 11 : 5015814,

6.4 Proof of Concept

- Aucun exploit n'est disponible pour le moment en sources ouvertes.

7 AZURE CVE-2022-33674

7.1 Résumé

Signalée par un agent anonyme, la CVE-2022-33674 est une vulnérabilité importante qui concerne Azure Site Recovery de Microsoft.

Solution native pour la reprise d'activité (DRaaS), Azure Site Recovery est dédiée au maintien des capacités opérationnelles d'une organisation lorsque celle-ci endure une situation de crise informatique majeure.

Selon Cybersecurity-Help, une restriction insuffisante de sécurité aurait été identifiée dans le produit Azure Site Recovery. Ce manque de restriction peut permettre à un attaquant non authentifié de contourner la politique de sécurité afin d'élever ses privilèges.

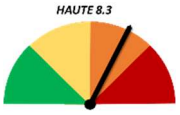
IBM X-Force indique que l'utilisation d'un programme malveillant est nécessaire pour réaliser l'exploit. Par ailleurs, il est aussi précisé que le risque est une exécution de code arbitraire avec les privilèges les plus élevés.

Point important : l'exploitation est réalisée via un vecteur d'attaque adjacent, impliquant que l'attaquant soit présent sur un réseau partagé. Une explication du vecteur d'attaque est proposée par Help-Prohacktive : « Le composant vulnérable est lié à la pile réseau, mais l'attaque est limitée au niveau du protocole à une topologie logiquement adjacente. Cela peut signifier qu'une attaque doit être lancée à partir du même réseau partagé physique (par exemple, Bluetooth ou IEEE 802.11) ou logique (par exemple, sous-réseau IP local), ou à partir d'un domaine administratif sécurisé ou autrement limité (par exemple, MPLS, VPN sécurisé pour une zone de réseau administratif). Un exemple d'attaque adjacente serait une inondation ARP (IPv4) ou de découverte de voisins (IPv6) conduisant à un déni de service sur le segment LAN local (par exemple, CVE-2013-6014) ».

7.2 Information

7.2.1 Risque

- Contournement de la politique de sécurité
- Exécution de code arbitraire (Selon IBM X-Force)
- Élévation de privilèges



7.2.2 Criticité

- La faille n'est pas activement exploitée
- Vecteur d'attaque : Adjacent
- Complexité d'attaque : Faible

- Privilèges requis : Aucun
- Interaction de l'utilisateur : Non
- Portée : Inchangée
- Impact sur la confidentialité : Haute
- Impact sur l'intégrité : Haute
- Impact sur la disponibilité : Faible

7.2.3 Composants vulnérables

- Microsoft Azure Site Recovery VMWare to Azure

7.3 Recommandation

- Une mise à jour de Microsoft existe. Le Patch Tuesday juillet 2022 apporte les correctifs nécessaires.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité du 12 juillet 2022, pour les produits concernés sont les suivantes.

- Le correctif cumulatif 62 pour Azure Site Recovery est disponible ici.

7.4 Proof of Concept

- Aucun exploit n'est disponible pour le moment en sources ouvertes.

8 Références

Microsoft

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-22047
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-30221
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-22038
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-22029
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-22039
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-22022
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-22041
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-30206
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-30226
- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2022-33674

IBM X-Force

- CVE-2022-22047:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229966
- CVE-2022-30221:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229938
- CVE-2022-22038:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229956
- CVE-2022-22029:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229951
- CVE-2022-22039:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229957
- CVE-2022-22022:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229944
- CVE-2022-22041:
  https://exchange.xforce.ibmcloud.com/vulnerabilities/229959

- CVE-2022-30206:

  https://exchange.xforce.ibmcloud.com/vulnerabilities/229928

- CVE-2022-30226:

  https://exchange.xforce.ibmcloud.com/vulnerabilities/229943

- CVE-2022-33674:

  https://exchange.xforce.ibmcloud.com/vulnerabilities/230000

Cybersecurity-help

- CVE-2022-22047:

  https://www.cybersecurity-help.cz/vdb/SB2022071220

- CVE-2022-30221:

  https://www.cybersecurity-help.cz/vdb/SB2022071228

- CVE-2022-22038:

  https://www.cybersecurity-help.cz/vdb/SB2022071231

- CVE-2022-22029 / 22039:

  https://www.cybersecurity-help.cz/vdb/SB2022071226

- CVE-2022-22022 / 22041 / 30206 / 30226:

  https://www.cybersecurity-help.cz/vdb/SB2022071233

- CVE-2022-33674:

  https://www.cybersecurity-help.cz/vdb/SB2022071222

Journaux

- https://krebsonsecurity.com/2022/07/microsoft-patch-tuesday-july-2022-edition/
- https://blog.qualys.com/vulnerabilities-threat-research/2022/07/12/july-2022-patch-tuesday
- https://www.tenable.com/blog/microsofts-july-2022-patch-tuesday-addresses-84-cves-cve-2022-22047
- https://help.prohacktive.io/lexique-cvss-000013-lang-fr.html
- http://www.mtom-mag.com/article12893.html
- https://www.kaspersky.fr/blog/printnightmare-vulnerability/17307/