aDvens

Security for the greater good

Renseignement sur les menaces
Patch Tuesday de janvier 2023

2023-01-11 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse

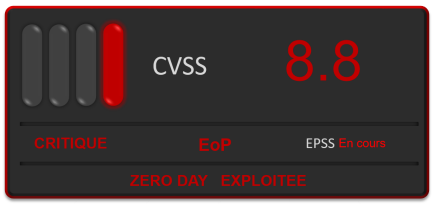
Le mercredi 11 janvier 2023, Microsoft a publié son bulletin mensuel ***Patch tuesday***, avec **98 failles** corrigées dont **1 zero day exploitée**: **CVE-2023-21674**.

Ce document aborde les vulnérabilités, ci-dessous, considérées comme les plus critiques :

PRODUIT	CVE	SCORE	EPSS	ZERO-DAY	EXPLOITEE	CWE	POC
ALPC	CVE-2023-21674	8.8 critique	En cours	Oui	Oui	119	Non
Service Cryptographique	CVE-2023-21561	8.8 critique	En cours	Non	Non	264	Non
SSTP	CVE-2023-21548	8.1 critique	En cours	Non	Non	362	Non
SSTP	CVE-2023-21535	8.1 critique	En cours	Non	Non	362	Non
L2TP	CVE-2023-21556	8.1 critique	En cours	Non	Non	416	Non
L2TP	CVE-2023-21555	8.1 critique	En cours	Non	Non	416	Non
L2TP	CVE-2023-21546	8.1 critique	En cours	Non	Non	416	Non
L2TP	CVE-2023-21543	8.1 critique	En cours	Non	Non	119	Non
L2TP	CVE-2023-21679	8.1 critique	En cours	Non	Non	416	Non
Service Cryptographique	CVE-2023-21730	7.8 critique	En cours	Non	Non	264	Non
Service Cryptographique	CVE-2023-21551	7.8 critique	En cours	Non	Non	264	Non
Sharepoint	CVE-2023-21743	5.3 critique	En cours	Non	Non	254	Non

2. Windows Advanced Local Procedure Call (ALPC) CVE-2023-21674 (Zero day - Exploitée)

2.1. Résumé



Découverte par des chercheurs d'Avast, la seule zero-day de ce *patch Tuesday* affecte le composant *Advanced Local Procedure Call* (ALPC) de Windows.

Cette fonctionnalité est employée par certaines applications Windows comme :

- les *RPCs* (*Remote Procedure Calls*),
- le *Winlogon* pour communiquer avec le *LSASS* (*Local Security Authentication Server Process*)
- certaines API envoyant des messages vers le processus sous-système de Windows.

Cette vulnérabilité permet à un attaquant local de s'échapper d'une sandbox Chromium et d'élever ses privilèges pour obtenir les privilèges **SYSTEM**.

Cette vulnérabilité est exploitée.

2.2. Informations

2.2.1. Risque

- Élévation de privilèges
- Changement de contexte

2.2.2. Type de vulnérabilité

- CWE-119 : Improper Restriction of Operations within the Bounds of a Memory Buffer.

2.2.3. Criticité

Vecteur d'attaque	Local	Interaction de l'utilisateur	Non	Impact sur l'intégrité	Fort
Complexité d'attaque	Faible	Portée	Changée	Impact sur la disponibilité	Fort
Privilèges requis	Faible	Impact sur la confidentialité	Fort		

2.2.4. Composants vulnérables

- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

2.2.5. Recommandations

Le patch Tuesday du mois de janvier 2023 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

2.2.6. Produits concernés et mises à jour à appliquer

KB5022346

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems

KB5022289

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

KB5022297

- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems

- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

2.2.7. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

3. Services de chiffrement Microsoft CVE-2022-21561

3.1. Résumé

L'équipe MORSE (*Microsoft Offensive Research and Security Engineering*) a découvert une vulnérabilité affectant spécifiquement les services de chiffrement Microsoft (CryptSvc), intégrés aux systèmes d'exploitation Windows.

Cette faille permet de contourner la politique de sécurité mise en place par la Sandbox *AppContainer*. Un attaquant, authentifié et connecté localement sur le système, peut envoyer des requêtes au service *CSRSS*, qui lui permettront de s'échapper de cette sandbox et d'obtenir les droits **SYSTEM**.

3.2. Informations

3.2.1. Risque

- Contournement de la politique de sécurité.
- Élévation de privilèges.

3.2.2. Type de vulnérabilité

- **CWE-264** : Permissions, Privileges, and Access Controls.

3.2.3. Criticité

Vecteur d'attaque : Local	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Changée	Impact sur la disponibilité : Fort
Privilèges requis : Faible	Impact sur la confidentialité : Fort	

3.2.4. Composants vulnérables

- Windows 7
- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

3.2.5. Recommandations

Le patch Tuesday du mois de janvier 2023 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

3.2.6. Produits concernés et mises à jour à appliquer

KB5022346

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems

KB5022343

- Windows Server 2012 (Server Core installation)
- Windows Server 2012

KB5022339

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1

KB5022353

- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

KB5022289

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems

- Windows 10 Version 1607 for 32-bit Systems

KB5022297

- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

3.2.7. Preuve de concept

Aucun exploit n'est disponible en sources ouvertes.

4. SSTP CVE-2023-21548 / 21535

4.1. Résumé

Disponible depuis le système d'exploitation Vista de Microsoft, Secure Socket Tunneling Protocol (SSTP) est un tunnel VPN qui permet d'initier une communication sécurisée via le protocole *PPP* (Point-to-Point Protocol).

Les chercheurs Yuki Chen et Cyber Kunlun ont identifié deux vulnérabilités dans ce protocole, de type *race condition* ou *situation de concurence*.

Une situation de concurrence peut se manifester lorsqu'une ressource est partagée, sans précaution, entre plusieurs tâches.

L'exploitation de ces vulnérabilités par un attaquant, distant et non authentifié, permet l'exécution de code arbitraire sur le système ciblé.

- Pour la **CVE-2023-21548**, l'attaquant peut forger une requête contenant du code malveillant et l'envoyer vers le serveur *RAS*.
- Pour la **CVE-2023-21535**, l'attaquant peut forger un paquet contenant du code malveillant et l'envoyer vers le serveur *SSTP*.

Microsoft précise que l'exploitation ne peut être réalisée uniquement si **l'attaquant remporte une situation de concurrence**.

4.2. Informations

4.2.1. Risque

- Exécution de code arbitraire à distance.

4.2.2. Type de vulnérabilité

- **CWE-362**: Concurrent Execution using Shared Resource with Improper Synchronization (Race Condition).

4.2.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Haute	Portée : Inchangée	Impact sur la disponibilité : Fort
Privilèges requis : Aucun	Impact sur la confidentialité : Fort	

4.2.4. Composants vulnérables

Pour la CVE-2023-21548

- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2022 Datacenter: Azure Edition

Pour la CVE-2023-21535

- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2022 Datacenter: Azure Edition

4.2.5. Recommandations

Le patch Tuesday du mois de janvier 2023 apporte les correctifs nécessaires.

Pour la **CVE-2023-21548**, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la **CVE-2023-21535**, des informations complémentaires sont disponibles sur le site de l'éditeur.

4.2.6. Produits concernés et mises à jour à appliquer

Pour la CVE-2023-21548

KB5022346

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems

KB5022343

- Windows Server 2012 (Server Core installation)
- Windows Server 2012

KB5022339

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1

KB5022353

- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

KB5022289

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

KB5022297

- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems

- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

Pour la CVE-2023-21535

KB5022346

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems

KB5022343

- Windows Server 2012 (Server Core installation)
- Windows Server 2012

KB5022353

- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

KB5022289

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

KB5022297

- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems

- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

4.2.7. Preuve de concept

Aucun exploit (POC) n'est disponible en sources ouvertes.

5. L2TP CVE-2023-21556 / 24555 / 21543 / 21546 / 21679

5.1. Résumé

Le chercheur Yuki Chen, en collaboration avec d'autres experts, a identifié cinq vulnérabilités dans le protocole *L2TP* présentant un défaut de traitement des données.

Il est possible pour un attaquant, distant et non authentifié, de forger des requêtes qui contiennent une charge utile déclenchée lors du traitement des données par le serveur RAS.

Le code malveillant est exécuté sur le serveur ciblé.

Microsoft précise que l'exploitation de ces cinq failles ne peut être réalisée uniquement si **l'attaquant remporte une situation de concurrence**.

5.2. Informations

5.2.1. Risque

- Exécution de code arbitraire à distance.

5.2.2. Types de vulnérabilités

Pour les CVE-2023-21556 / 24555 / 21546 / 21679

- CWE-416: Use After Free.

Pour la CVE-2023-21543

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer.

Pour les CVE-2023-21556 / 24555 / 21543 / 21546 / 21679

- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization (Race Condition).

5.2.3. Criticité

Vecteur d'attaque	Réseau	Interaction de l'utilisateur	Non	Impact sur l'intégrité	Fort
Complexité d'attaque	Haute	Portée	Inchangée	Impact sur la disponibilité	Fort
Privilèges requis	Aucun	Impact sur la confidentialité	Fort		

5.2.4. Composants vulnérables

- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2022 Datacenter: Azure Edition

5.2.5. Recommandations

Le patch Tuesday du mois de janvier 2023 apporte les correctifs nécessaires.

Pour la **CVE-2023-21556**, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la **CVE-2023-21555**, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la **CVE-2023-21546**, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la **CVE-2023-21543**, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la **CVE-2023-21679**, des informations complémentaires sont disponibles sur le site de l'éditeur.

5.2.6. Produits concernés et mises à jour à appliquer

KB5022346

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems

KB5022343

- Windows Server 2012 (Server Core installation)

- Windows Server 2012

KB5022339

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1

KB5022353

- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

KB5022289

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

KB5022297

- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems

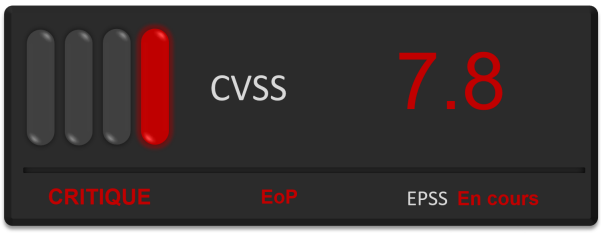
- Windows 10 Version 1809 for 32-bit Systems

5.2.7. Preuve de concept

Aucun exploit (POC) n'est disponible en sources ouvertes.

6. Services de chiffrement Microsoft CVE-2023-21551 / 21730

6.1. Résumé



Découvertes par l'équipe MORSE (*Microsoft Offensive Research and Security Engineering*), il s'agit de deux vulnérabilités critiques qui affectent le service cryptographique de Microsoft.

Les chercheurs ont identifié un défaut de gestion des permissions permettant à un attaquant, authentifié en tant que simple utilisateur, de contourner la politique de sécurité pour élever ses privilèges sur le système.

6.2. Informations

6.2.1. Risque

- Contournement de la politique de sécurité.
- Élévation de privilèges.

6.2.2. Type de vulnérabilité

- CWE-264: Permissions, Privileges, and Access Controls.

6.2.3. Criticité

Vecteur d'attaque : Local	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Inchangée	Impact sur la disponibilité : Fort
Privilèges requis : Faible	Impact sur la confidentialité : Fort	

6.2.4. Composants vulnérables

Pour la CVE-2023-21551

- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2022 Datacenter: Azure Edition

Pour la CVE-2023-21730

- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2022 Datacenter: Azure Edition

Listes des produits dépendants

- Microsoft Windows Server 2008

6.2.5. Recommandations

Le patch Tuesday du mois de janvier 2023 apporte les correctifs nécessaires.

Pour la **CVE-2023-21551**, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la **CVE-2023-21730**, des informations complémentaires sont disponibles sur le site de l'éditeur.

6.2.6. Produits concernés et mises à jour à appliquer

Pour la CVE-2023-21551

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

Pour la CVE-2023-21730

KB5022346

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems

KB5022343

- Windows Server 2012 (Server Core installation)
- Windows Server 2012

KB5022339

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1

KB5022353

- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

KB5022289

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

KB5022297

- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems

KB5022282

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems

KB5022303

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5022287

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5022291

- Windows Server 2022 (Server Core installation)
- Windows Server 2022

KB5022286

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

6.2.7. Preuve de concept

Aucun exploit (POC) n'est disponible en sources ouvertes.

7. SharePoint CVE-2022-21743

7.1. Résumé

Un contournement de la fonctionnalité de sécurité (SFB) affecte *Microsoft SharePoint*. L'exploitation de cette vulnérabilité permet à un attaquant non authentifié de contourner l'authentification, puis d'établir une connexion anonyme à un serveur SharePoint.

7.2. Informations

7.2.1. Risque

- Contournement de la politique de sécurité du système.

7.2.2. Type de vulnérabilité

- **CWE-254** : I7PK - Security Features.

7.2.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Faible
Complexité d'attaque : Faible	Portée : Inchangée	Impact sur la disponibilité : Aucun
Privilèges requis : Aucun	Impact sur la confidentialité : Aucun	

7.2.4. Composants vulnérables

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016

7.3. Recommandations

Le patch Tuesday du mois de janvier 2023 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour sécuriser un serveur Sharepoint, une mise à niveau peut être effectuée en exécutant soit :

- l'assistant de configuration des produits SharePoint,
- l'applet de commande Upgrade-SPFarm PowerShell
- la commande *psconfig.exe -cmd upgrade -inplace b2b* après l'installation de la mise à jour.

7.3.1. Produits concernés et mises à jour à appliquer

KB5002331

- Microsoft SharePoint Server Subscription Edition

KB5002329

- Microsoft SharePoint Server 2019

KB5002338

- Microsoft SharePoint Enterprise Server 2016

7.3.2. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

8. Références

Articles

- https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2023-patch-tuesday-fixes-98-flaws-1-zero-day/
- https://www.zerodayinitiative.com/blog/2023/1/10/the-january-2023-security-update-review

ALPC CVE-2023-21674

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21674
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243184
- https://www.cybersecurity-help.cz/vdb/SB2023011042

CRYPTOGRAPHIC SERVICES CVE-2023-21730

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21730
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243200
- https://www.cybersecurity-help.cz/vdb/SB2023011054

CRYPTOGRAPHIC SERVICES CVE-2023-21551

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21551
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243133
- https://www.cybersecurity-help.cz/vdb/SB2023011054

CRYPTOGRAPHIC SERVICES CVE-2023-21561

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21561
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243182
- https://www.cybersecurity-help.cz/vdb/SB2023011054

SHAREPOINT CVE-2023-21743

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21743
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243211
- https://www.cybersecurity-help.cz/vdb/SB2023011051

SSTP CVE-2023-21548

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21548
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243129
- https://www.cybersecurity-help.cz/vdb/SB2023011101

SSTP CVE-2023-21535

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21535
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243120

- https://www.cybersecurity-help.cz/vdb/SB2023011101

L2TP CVE-2023-21556

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21556
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243136
- https://www.cybersecurity-help.cz/vdb/SB2023011048

L2TP CVE-2023-21555

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21555
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243135
- https://www.cybersecurity-help.cz/vdb/SB2023011048

L2TP CVE-2023-21546

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21546
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243122
- https://www.cybersecurity-help.cz/vdb/SB2023011048

L2TP CVE-2023-21543

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21543
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243128
- https://www.cybersecurity-help.cz/vdb/SB2023011048

L2TP CVE-2023-21679

- https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-21679
- https://exchange.xforce.ibmcloud.com/vulnerabilities/243188
- https://www.cybersecurity-help.cz/vdb/SB2023011048