aDvens

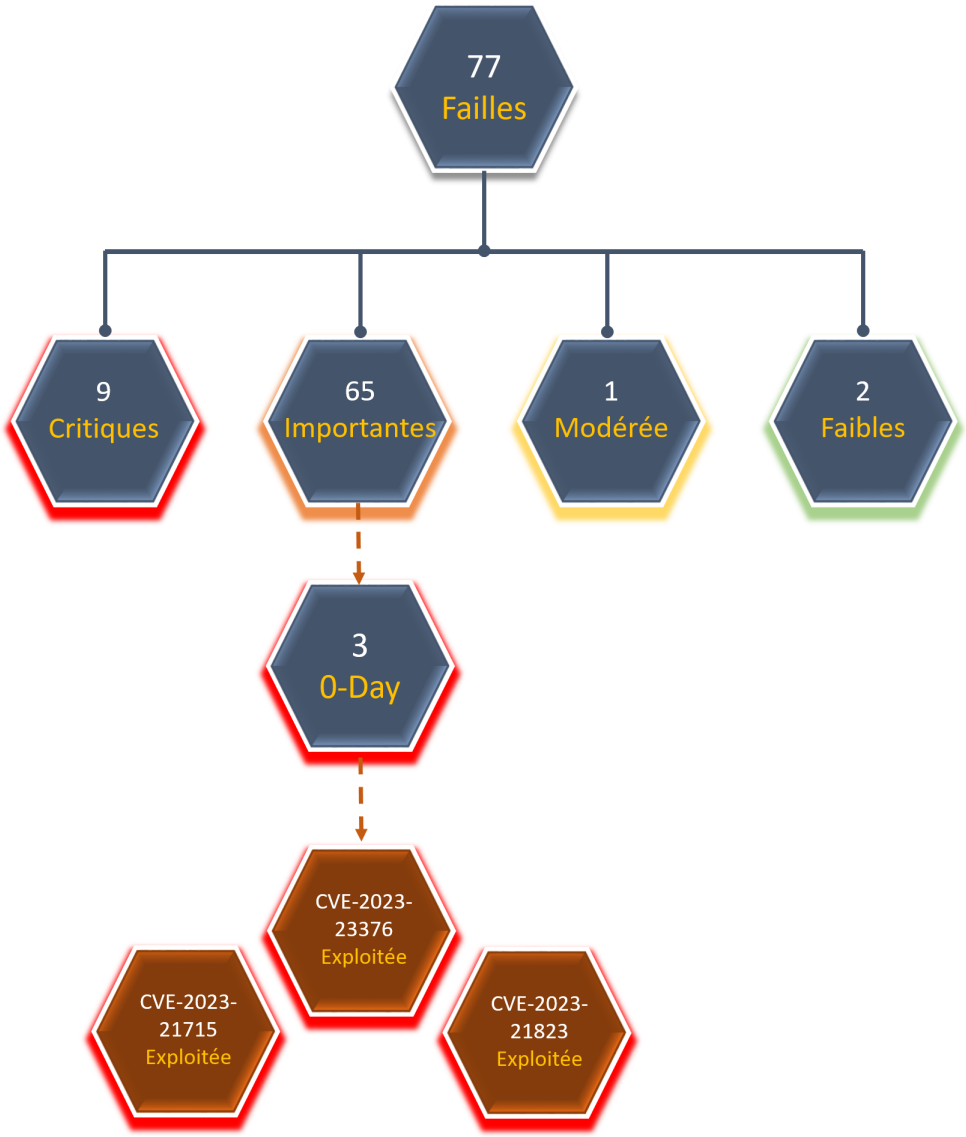
Security for the greater good

Renseignement sur les menaces
Patch Tuesday de février 2023

2023-02-15 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse



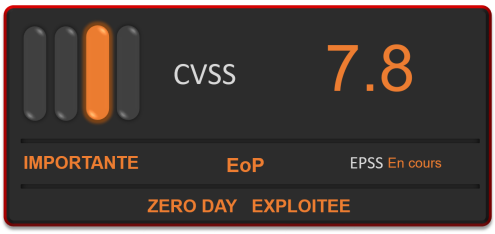
Le mercredi 14 février 2023, Microsoft a publié son bulletin mensuel ***Patch tuesday***, avec **77 failles** corrigées dont **3 zero day exploitées**: **CVE-2023-23376**, **CVE-2023-21823** et **CVE-2023-21715**.

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

PRODUIT	CVE	SCORE	EPSS	ZERO-DAY	EXPLOITEE	CWE	POC
Microsoft Common Log	CVE-2023-23376	7.8 Importante	En cours	Oui	Oui	119	Non
Windows Graphics	CVE-2023-21823	7.8 Importante	En cours	Oui	Oui	119	Non
Microsoft Publisher	CVE-2023-21715	7.3 Importante	En cours	Oui	Oui	254	Non
Microsoft Word	CVE-2023-21716	9.8 Critique	En cours	Non	Non	120	Non
Windows iSCSI	CVE-2023-21803	9.8 Critique	En cours	Non	Non	20	Non
Windows Protected EAP (PEAP)	CVE-2023-21692	9.8 Critique	En cours	Non	Non	20	Non
Windows Protected EAP (PEAP)	CVE-2023-21690	9.8 Critique	En cours	Non	Non	20	Non
Windows Protected EAP (PEAP)	CVE-2023-21689	9.8 Critique	En cours	Non	Non	20	Non
Net et Visual Studio Code	CVE-2023-21808	8.4 Critique	En cours	Non	Non	20	Non
Visual Studio Code	CVE-2023-21815	8.4 Critique	En cours	Non	Non	119	Non
Visual Studio Code	CVE-2023-23381	8.4 Critique	En cours	Non	Non	119	Non
Serveur SQL	CVE-2023-21718	7.8 Critique	En cours	Non	Non	20	Non

2. Windows Common Log File System Driver CVE-2023-23376 (Zero day - Exploitée)

2.1. Résumé



Découverte par des chercheurs en sécurité de Microsoft, cette zero-day affecte le composant *Common Log File System* (*CLFS*) de Windows.

Cette fonctionnalité permet aux applications en mode *noyau* et *utilisateur* de générer et sauvegarder des journaux d'activité.

La vulnérabilité permet à un attaquant local d'élever ses privilèges pour obtenir les droits **SYSTEM**.

Cette vulnérabilité est exploitée.

2.2. Informations

2.2.1. Risque

- Élévation de privilèges

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	Inchangée	Impact sur la disponibilité	Fort
Privilèges requis	Faible	Impact sur la confidentialité	Fort		

2.2.4. Composants vulnérables

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

2.2.5. Recommandations

Le patch Tuesday du mois de février 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

KB5022838

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

KB5022858

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

KB5022840

- 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

KB5022834

- 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 ARM64-based Systems
- Windows 10 Version 21H2 for x64-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

KB5022845

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

KB5022836

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

KB5022842

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

KB5022899

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022894

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022903

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

KB5022895

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

KB5022872

- 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

KB5022874

- 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

KB5022890

- 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 x32-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x32-based Systems Service Pack 2

KB5022893

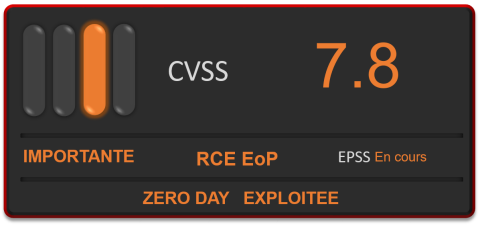
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x32-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x32-based Systems Service Pack 2

2.2.7. Preuve de concept

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

3. Windows Graphics CVE-2023-21823

3.1. Résumé



Dhanesh Kizhakkinan et Genwei Jiang de l'équipe Mandiant ont découvert une vulnérabilité affectant le composant graphique de Windows.

Cette faille permet à un attaquant authentifié et connecté localement sur le système, d'exécuter du code arbitraire avec les privilèges **SYSTEM**.

Cette vulnérabilité est exploitée.

3.2. Informations

3.2.1. Risque

- Exécution de code arbitraire à distance.
- Élévation de privilèges.

3.2.2. Type de vulnérabilité

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

3.2.3. 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	

3.2.4. Composants vulnérables

- Windows 10
- Windows 11

- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Microsoft Office pour iOS
- Microsoft Office pour Universal
- Microsoft Office pour Android

3.2.5. Recommandations

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

Les mises à jour s'effectue automatiquement à partir du Windows Store et non à partir des mises à jour Windows.
Si les mises à jour automatiques du Windows store ont été désactivées, il faudra les effectuer manuellement (guide microsoft)

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

3.2.6. Produits concernés et mises à jour à appliquer

KB5022838

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

KB5022858

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

KB5022840

- 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

KB5022834

- 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 ARM64-based Systems
- Windows 10 Version 21H2 for x64-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

KB5022845

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

KB5022836

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

KB5022842

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

KB5022899

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022894

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022903

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

KB5022895

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

KB5022872

- 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

KB5022874

- 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

KB5022890

- 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 x32-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x32-based Systems Service Pack 2

KB5022893

- 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 x32-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x32-based Systems Service Pack 2

Support App Store

- Microsoft Office pour iOS

Support Microsoft Store

- Microsoft Office pour Universal

Support Play Store

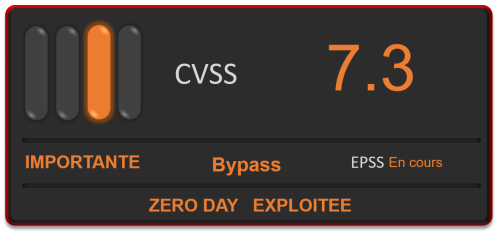
- Microsoft Office pour Android

3.2.7. Preuve de concept

Aucun exploit n'est disponible en sources ouvertes.

4. Microsoft Publisher CVE-2023-21715

4.1. Résumé



Le chercheur Hidetake Jo a identifié une vulnérabilité lors du traitement de macros Office par Publisher.

Un attaquant peut contourner les politiques de blocage et exécuter une macro office via un document Publisher forgé, sans interagir avec l'utilisateur.

Microsoft précise que l'exploitation ne peut être réalisée uniquement si **l'attaquant est authentifié et connecté localement** sur le système.

Cette vulnérabilité est exploitée.

4.2. Informations

4.2.1. Risque

- Contournement de la politique de sécurité.

4.2.2. Type de vulnérabilité

- CWE-254: 7PK - Security Features.

4.2.3. Criticité

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

4.2.4. Composants vulnérables

- Applications Microsoft 365 pour des systèmes 32-bits
- Applications Microsoft 365 pour des systèmes 64-bits

4.2.5. Recommandations

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

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

4.2.6. Produits concernés et mises à jour à appliquer

Mises à jour Microsoft Office

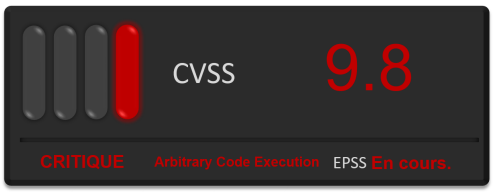
- Applications Microsoft 365 pour des systèmes 32-bits
- Applications Microsoft 365 pour des systèmes 64-bits

4.2.7. Preuve de concept

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

5. Microsoft Word CVE-2023-21716

5.1. Résumé



Une vulnérabilité critique a été découverte dans Microsoft Word. Cette faille affecte également le *Preview Pane* d'Outlook.

Il est possible pour un attaquant, distant et non authentifié, d'envoyer un mail contenant une charge utile au format *RTF* pour exécuter du code arbitraire avec les droits de la victime.

5.2. Informations

5.2.1. Risque

- Exécution de code arbitraire.

5.2.2. Type de vulnérabilité

- CWE-120 : buffer copy without checking size of input ("classic buffer overflow").

5.2.3. Criticité

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

5.2.4. Composants vulnérables

- Microsoft Word 2013
- Microsoft Word 2016
- Microsoft Office 2019
- Microsoft Office Online Server
- Microsoft Sharepoint 2013
- Microsoft Sharepoint 2016
- Microsoft Sharepoint 2019

- Microsoft 365 Apps for Entreprise
- Microsoft Office LTSC 2021
- Microsoft Office LTSC pour Mac 2021

5.2.5. Recommandations

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

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

5.2.6. Produits concernés et mises à jour à appliquer

KB5002316

- Microsoft Word 2013 Service Pack 1 (64-bit editions)
- Microsoft Word 2013 RT Service Pack 1
- Microsoft Word 2013 Service Pack 1 (32-bit editions)

KB5002347

- Microsoft SharePoint Foundation 2013 Service Pack 1

KB5002312

- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1

KB5002313

- Microsoft Office Web Apps Server 2013 Service Pack 1

KB5002323

- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)

KB5002342

- Microsoft SharePoint Server 2019

KB5002330

- Microsoft SharePoint Server 2019

KB5002346

- Microsoft SharePoint Enterprise Server 2013 Service Pack 1

KB5002347

- Microsoft SharePoint Enterprise Server 2013 Service Pack 1

KB5002325

- Microsoft SharePoint Enterprise Server 2016

KB5002309

- Microsoft Office Online Server

KB5002352

- SharePoint Server Subscription Edition Language Pack
- Microsoft SharePoint Server Subscription Edition

KB5002353

- Microsoft SharePoint Server Subscription Edition

Mises à jour Microsoft Office

- Applications Microsoft 365 pour des systèmes 32-bits
- Applications Microsoft 365 pour des systèmes 64-bits
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft Office LTSC 2021 for 32-bit editions

Informations Mac

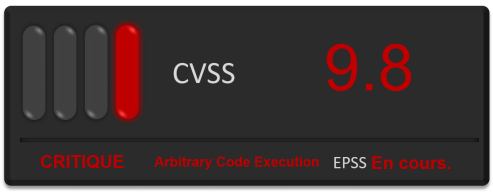
- Microsoft Office 2019 for Mac
- Microsoft Office LTSC for Mac 2021

5.2.7. Preuve de concept

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

6. Microsoft iSCSI CVE-2023-21803

6.1. Résumé



Découverte par le chercheur Azure Yang du laboratoire *Kunlun Lab*, cette vulnérabilité critique affecte la technologie iSCSI (*Internet Small Computer System Interface*).

Développée en 1998 par IBM, la technologie iSCSI permet de transporter de données entre un initiateur iSCSI, installé sur un serveur, et une cible iSCSI, installée sur un dispositif de stockage.

Le chercheur a identifié un contrôle insuffisant des données insérées par l'utilisateur.

L'exploitation de cette faille permet à un attaquant distant, en envoyant des requêtes DHCP malveillantes vers le service *iSCSI Discovery*, d'exécuter du code arbitraire sur le système.

Microsoft précise que seulement les versions x86 et 32-bits de Windows sont concernées par cette vulnérabilité.

6.2. Informations

6.2.1. Risque

- Exécution de code arbitraire.

6.2.2. Type de vulnérabilité

- CWE-20: Improper Input Validation.

6.2.3. Criticité

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

6.2.4. Composants vulnérables

- Microsoft Windows 10
- Microsoft Windows Server 2008

6.2.5. Recommandations

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

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

6.2.6. Atténuation

Microsoft précise que l'initiateur iSCSI de l'application client est désactivé par défaut. L'exploitation de la vulnérabilité n'est possible que si ce dernier est activé.

6.2.7. Produits concernés et mises à jour à appliquer

KB5022890

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

KB5022893

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

KB5022838

- Windows 10 Version 1607 for 32-bit Systems

KB5022858

- Windows 10 for 32-bit Systems

KB5022834

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

KB5022840

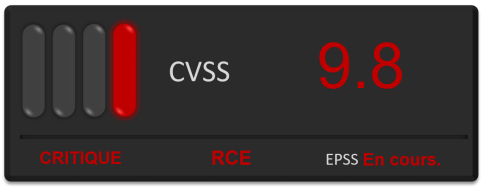
- Windows 10 Version 1809 for 32-bit Systems

6.2.8. Preuve de concept

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

7. Microsoft EAP (PEAP) CVE-2023-21692 / 21690 / 21689

7.1. Résumé



Trois vulnérabilités critiques dans le protocole PEAP (*Protected Extensible Authentication Protocol*) ont été découvertes par les chercheurs Yuki Chen et Jarvis_1oop.

Développé conjointement par Microsoft, RSA Security et Cisco Systems, le protocole PEAP permet de réaliser des transferts sécurisés d'informations d'authentification.

Les chercheurs ont constaté que le contrôle des données insérées est insuffisant. Il est ainsi possible pour un attaquant, distant et non authentifié, d'envoyer des paquets PEAP forgés afin d'exécuter du code arbitraire sur le système.

L'exploitation nécessite que NPS sur le serveur Windows soit actif et que la politique de réseau autorise le protocole PEAP.

7.2. Informations

7.2.1. Risque

- Exécution de code arbitraire à distance.

7.2.2. Type de vulnérabilité

- CWE-20: Improper Input Validation.

7.2.3. Criticité

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

7.2.4. Composants vulnérables

Pour la CVE-2023-21689

- 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

Pour la CVE-2023-21690

- 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

Pour la CVE-2023-21692

- 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

7.2.5. Recommandations

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

Pour la CVE-2023-21689, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la CVE-2023-21690, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la CVE-2023-21692, des informations complémentaires sont disponibles sur le site de l'éditeur.

7.2.6. Atténuation

Microsoft propose une solution d'atténuation:

Le protocole PEAP (*Protected Extensible Authentication Protocol*) de Microsoft n'est négocié avec le client que si NPS est exécuté sur le serveur Windows et qu'une stratégie réseau autorisant *PEAP* est configurée.

Pour désactiver ce protocole, vous devez veiller à ce que le type *PEAP* ne soit pas configuré en tant que type *EAP* autorisé dans votre stratégie réseau.

Pour en savoir plus, consultez la section Configurer la nouvelle stratégie de réseau sans fil et l'article Configurer des stratégies réseau.

7.2.7. Produits concernés et mises à jour à appliquer

Pour la CVE-2023-21689

KB5022838

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

KB5022858

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

KB5022840

- 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

KB5022834

- 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 ARM64-based Systems
- Windows 10 Version 21H2 for x64-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

KB5022845

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

KB5022836

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

KB5022842

- Windows Server 2022 (Server Core installation)

- Windows Server 2022

KB5022899

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022894

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022903

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

KB5022895

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

KB5022872

- 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

KB5022874

- 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

Pour la CVE-2023-21690

KB5022838

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

KB5022858

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

KB5022834

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

KB5022845

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

KB5022836

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

- Windows 10 Version 20H2 for ARM64-based Systems

KB5022842

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

KB5022840

- 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

KB5022899

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022894

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022903

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

KB5022895

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

KB5022872

- 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

KB5022874

- 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

Pour la CVE-2023-21692

KB5022840

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

KB5022890

- 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

KB5022893

- 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

KB5022834

- Windows 10 Version 22H2 for x64-based Systems

KB5022845

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

KB5022834

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

KB5022836

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

KB5022872

- Windows Server 2008 R2 for x64-based Systems Service Pack 1

KB5022874

- Windows Server 2008 R2 for x64-based Systems Service Pack 1

KB5022890

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

KB5022893

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

KB5022899

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022894

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

KB5022903

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

KB5022895

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

KB5022872

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

KB5022874

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

KB5022834

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

KB5022842

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

KB5022838

- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

KB5022858

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

KB5022834

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

7.2.8. Preuve de concept

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

8. Microsoft .NET et Visual Studio Code CVE-2023-21808 / 21815 / 23381

8.1. Résumé

Plusieurs vulnérabilités affectant *Microsoft .NET Framework* et *Visual Studio Code* ont été découvertes.

Parmi elles, les trois failles les plus critiques sont :

- la CVE-2023-21808, avec un contrôle insuffisant des données insérées par l'utilisateur ;
- la CVE-2023-21815 et la CVE-2023-23381, avec un défaut de limitation des données traitées ;

Un attaquant distant, et non authentifié peut exploiter ces vulnérabilités, en utilisant des données forgées, afin d'exécuter du code arbitraire sur le système.

Microsoft précise que le vecteur d'attaque est local. En effet, bien que l'attaquant soit distant, l'exécution du code arbitraire est exécutée localement sur le système de la victime.

8.2. Informations

8.2.1. Risque

- Exécution de code arbitraire à distance.

8.2.2. Type de vulnérabilité

Pour la CVE-2023-21808

CWE-20: Improper Input Validation.

Pour la CVE-2023-21815 et la CVE-2023-23381

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

8.2.3. 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 : Aucun	Impact sur la confidentialité : Fort	

8.2.4. Composants vulnérables

Pour la CVE-2023-21808

- Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 32-bit Systems Service Pack 2
- Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 X64-based Systems Service Pack 2
- Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 32-bit Systems Service Pack 2
- Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 x64-based Systems Service Pack 2
- Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 32-bit Systems 1809
- Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 ARM64-based Systems 1809
- Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 X64-based Systems 1809
- Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 32-bit Systems 1809
- Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 32-bit Systems 20H2
- Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 ARM64-based Systems 20H2
- Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 X64-based Systems 1809
- Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 X64-based Systems 20H2
- Microsoft Visual Studio 2017 15.9
- Microsoft Visual Studio 2019 16.11
- Microsoft Visual Studio 2022 17.0
- Microsoft Visual Studio 2022 17.2
- Microsoft Visual Studio 2022 17.4

Pour la CVE-2023-21815 et la CVE-2023-23381

- Microsoft Visual Studio 2017 15.9
- Microsoft Visual Studio 2019 16.11
- Microsoft Visual Studio 2022 17.0
- Microsoft Visual Studio 2022 17.2
- Microsoft Visual Studio 2022 17.4

8.2.5. Recommandations

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

Pour la CVE-2023-21808, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la CVE-2023-21815, des informations complémentaires sont disponibles sur le site de l'éditeur.

Pour la CVE-2023-23381, des informations complémentaires sont disponibles sur le site de l'éditeur.

8.2.6. Produits concernés et mises à jour à appliquer

Pour la CVE-2023-21808

KB5022858

- Microsoft .NET Framework 3.5 and 4.6.2

KB5023288

- NET 6.0

KB5022729

- Microsoft .NET Framework 3.5 AND 4.8
- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022838

- Microsoft .NET Framework 3.5 AND 4.7.2
- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022503

- Microsoft .NET Framework 3.5 AND 4.8

KB5022732

- Microsoft .NET Framework 4.

KB5022784

- Microsoft .NET Framework 4.8

KB5022727

- Microsoft .NET Framework 3.5 AND 4.8

KB5022782

- Microsoft .NET Framework 3.5 AND 4

KB5022731

- Microsoft .NET Framework 4.8

KB5022783

- Microsoft .NET Framework 4.8

KB5022858

- Microsoft .NET Framework 3.5 and 4.6.2

KB5022734

- Microsoft .NET Framework 4.6.2

KB5022786

- Microsoft .NET Framework 4.6.2

KB5022497

- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022730

- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022728

- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022727

- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022735

- Microsoft .NET Framework 3.5 AND 4.8.1

KB5022732

- Microsoft .NET Framework 4.8

KB5022784

- Microsoft .NET Framework 4.8

KB5022731

- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2

KB5022783

- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2

KB5022733

- Microsoft .NET Framework 4.8
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2

KB5022785

- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2

Notes de version

- Microsoft Visual Studio 2022 version 17.4

Notes de version

- Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)

Notes de version

- Microsoft Visual Studio 2022 version 17.2

Notes de version

- Microsoft Visual Studio 2022 version 17.0

Notes de version

- Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)

Pour la CVE-2023-21815 et la CVE-2023-23381

Notes de version

- Microsoft Visual Studio 2022 version 17.4

Notes de version

- Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)

Notes de version

- Microsoft Visual Studio 2022 version 17.2

Notes de version

- Microsoft Visual Studio 2022 version 17.0

Notes de version

- Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)

8.2.7. Preuve de concept

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

9. Microsoft serveur SQL CVE-2023-21718

9.1. Résumé

La CVE-2023-21718 est une vulnérabilité critique qui affecte le serveur SQL de Microsoft.

La faille concerne un contrôle insuffisant des données traitées.

Un attaquant peut inciter un utilisateur à s'authentifier, via l'intergiciel ODBC, à une base de données d'un serveur SQL compromis. Lors de l'authentification, les données récupérées depuis la base de données peuvent contenir du code arbitraire qui est exécuté sur le système client.

Une interaction avec l'utilisateur est obligatoire pour exécuter la charge utile.

9.2. Informations

9.2.1. Risque

- Exécution de code arbitraire.

9.2.2. Type de vulnérabilité

- **CWE-20**: Improper Input Validation.

9.2.3. Criticité

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

9.2.4. Composants vulnérables

- Microsoft SQL Server 2008
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014

- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft SQL Server 2022

9.2.5. Recommandations

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

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

9.2.6. Produits concernés et mises à jour à appliquer

KB5021124

- Microsoft SQL Server 2019 for x64-based Systems (CU 18)

KB5021522

- Microsoft SQL Server 2022 for x64-based Systems (GDR)

KB5021126

- Microsoft SQL Server 2017 for x64-based Systems (CU 31)

KB5021128

- Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connectivity Pack

KB5021129

- Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)

KB5021045

- Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)

KB5021125

- Microsoft SQL Server 2019 for x64-based Systems (GDR)

KB5021045

- Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)

KB5021037

- Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
- Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)

KB5021127

- Microsoft SQL Server 2017 for x64-based Systems (GDR)

9.2.7. Preuve de concept

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

10. Références

Articles

- https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/

Microsoft Graphics CVE-2023-21823

- https://exchange.xforce.ibmcloud.com/vulnerabilities/245994
- https://www.cybersecurity-help.cz/vdb/SB2023021420
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21823

Microsoft Publisher CVE-2023-21715

- https://exchange.xforce.ibmcloud.com/vulnerabilities/246016
- https://www.cybersecurity-help.cz/vdb/SB2023021418
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21715

Microsoft Common Log CVE-2023-23376

- https://exchange.xforce.ibmcloud.com/vulnerabilities/246033
- https://www.cybersecurity-help.cz/vdb/SB2023021419
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23376

Microsoft Word CVE-2023-21716

- https://exchange.xforce.ibmcloud.com/vulnerabilities/246017
- https://www.cybersecurity-help.cz/vdb/SB2023021433
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21716

Microsoft iSCSI CVE-2023-21803

- https://exchange.xforce.ibmcloud.com/vulnerabilities/245979
- https://www.cybersecurity-help.cz/vdb/SB2023021440
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21803

Microsoft EAP CVE-2023-21692

- https://exchange.xforce.ibmcloud.com/vulnerabilities/246002
- https://www.cybersecurity-help.cz/vdb/SB2023021436
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21692

Microsoft EAP CVE-2023-21690

- https://exchange.xforce.ibmcloud.com/vulnerabilities/246000
- https://www.cybersecurity-help.cz/vdb/SB2023021436
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21690

Microsoft EAP CVE-2023-21689

- https://exchange.xforce.ibmcloud.com/vulnerabilities/245999
- https://www.cybersecurity-help.cz/vdb/SB2023021436
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21689

Microsoft NET et Visual Studio CVE-2023-21808

- https://exchange.xforce.ibmcloud.com/vulnerabilities/245982
- https://www.cybersecurity-help.cz/vdb/SB2023021504
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21808

Visual Studio CVE-2023-21815

- https://exchange.xforce.ibmcloud.com/vulnerabilities/245987
- https://www.cybersecurity-help.cz/vdb/SB2023021505
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21815

Visual Studio CVE-2023-23381

- https://exchange.xforce.ibmcloud.com/vulnerabilities/246897
- https://www.cybersecurity-help.cz/vdb/SB2023021505
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23381

Microsoft Serveur SQL CVE-2023-21718

- https://exchange.xforce.ibmcloud.com/vulnerabilities/245959
- https://www.cybersecurity-help.cz/vdb/SB2023021426
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21718