NEWSCAST CYBER THREAT INTELLIGENCE

PATCH TUESDAY MICROSOFT MAI 2022

CERT ADVENS

11/05/2022 / TLP-WHITE

SOMMAIRE

01 PATCH TUESDAY MICROSOFT

Le 11 mai 2022, Microsoft a publié son Patch Tuesday dans lequel il annonce un ensemble de mises à jour pour plusieurs de ses produits. Ce patch apporte des correctifs pour un total de 75 vulnérabilités et 3 zero-day.

Parmi ces 75 vulnérabilités, il y a la CVE-2022-26925 qui est activement exploitée.

Ce bulletin se concentre sur les vulnérabilités ci-dessous

Windows LSA: CVE-2022-26925

Protocole PPTP (Point-to-Point Tunneling): CVE-2022-21972 CVE-2022-23270

Windows Kerberos: CVE-2022-26931

Active Directory Domain Service (AD DS): CVE-2022-26923

Windows Network File System: CVE-2022-26937

Remote Desktop Client: CVE-2022-22017

Microsoft Visual Studio: CVE-2022-30129

Microsoft Exchange Server: CVE-2022-21978

Windows ALPC: CVE-2022-23279

LDAP: CVE-2022-22012 CVE-2022-22013 CVE-2022-22014 CVE-2022-29128 CVE-2022-29129 CVE-2022-29130 CVE-2022-29131

Microsoft Print Spooler: CVE-2022-29104

Office Excel: CVE-2022-29109 CVE-2022-29110

02 CVE-2022-26925 (LSA)

02.1 RÉSUMÉ

La CVE-2022-26925 est une vulnérabilité qui peut être utilisée pour réaliser une attaque de type « relais NTLM ». Aussi connue sous l'appellation **PetitPotam**, ce type d'attaque utilise des relais NTLM malveillants afin de compromettre des serveurs contrôleurs de domaine Windows.

Le scénario de l'attaque est le suivant :

Dans un premier temps, un attaquant distant et non authentifié crée un relai NTLM frauduleux. L'attaquant utilise des appels de méthodes via l'interface LSARPC pour obliger le serveur contrôleur de domaine à venir s'authentifier vers le relai frauduleux. Le serveur va alors partager son certificat d'authentification avec le relai.

Dans un second temps, l'attaquant récupère depuis son relai le certificat d'authentification légitime et l'utilise à son tour pour s'authentifier vers le domaine Active Directory ciblé.

Cette vulnérabilité est activement exploitée mais aucun POC n'est disponible actuellement en sources ouvertes.

02.2 INFORMATIONS

02.2.1 | RISQUES

- Usurpation d'identité
- Élévation de privilèges
- Contournement de la politique de sécurité

02.2.2 | CRITICITE

- **La faille est 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**

02.2.3 | CVE

- CVE-2022-26925

02.2.4 | COMPOSANTS VULNERABLES.

- Microsoft Windows Server 2008 SP2 x32
- 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 for 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows Server version 20H2
- 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 for 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

02.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

02.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

03 CVE-2022-21972 (PPTP)

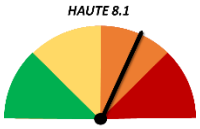
03.1 RÉSUMÉ

Une vulnérabilité de type « situation de concurrence (race condition)» a été identifiée dans le PPTP (Point-to-point Tunneling Protocol) de Microsoft.

L'exploitation de cette vulnérabilité par un attaquant distant et non authentifié utilisant une requête forgée, peut permettre l'exécution de code arbitraire sur le système.

03.2 INFORMATIONS

03.2.1 | RISQUES



- Exécution de code arbitraire (à distance)

03.2.2 | CRITICITE

- **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**

03.2.3 | CVE

- CVE-2022-21972

03.2.4 | COMPOSANTS VULNERABLES.

- 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 for 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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 for X64-based systems (Server Core installation) 2008 SP2
- Microsoft Windows Server for 32-bit systems (Server Core installation) 2008 SP2
- Microsoft Windows Server for 32-bit systems 2008 SP2
- Microsoft Windows Server for 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

03.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

03.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

04 CVE-2022-23270 (PPTP)

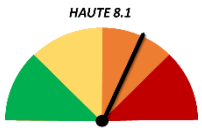
04.1 RÉSUMÉ

Une vulnérabilité de type « situation de concurrence (race condition)» a été identifiée dans le PPTP (Point-to-point Tunneling Protocol) de Microsoft.

L'exploitation de cette vulnérabilité par un attaquant distant et non authentifié utilisant une requête forgée, peut permettre l'exécution de code arbitraire sur le système.

04.2 INFORMATIONS

04.2.1 | RISQUES



- Exécution de code arbitraire (à distance)

04.2.2 | CRITICITE

- **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**

04.2.3 | CVE

- CVE-2022-23270

04.2.4 | COMPOSANTS VULNERABLES.

- Systems Produits concernés
- Microsoft Windows Server 2008 SP2 x32
- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 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 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 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

04.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

04.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

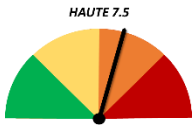
05 CVE-2022-26931 (KERBEROS)

05.1 RÉSUMÉ

Un défaut a été découvert dans le protocole d'authentification Kerberos du système d'exploitation Windows de Microsoft. Il est possible pour un attaquant distant et authentifié en tant que simple utilisateur d'utiliser une requête forgée afin d'exécuter de code arbitraire sur le système avec les privilèges les plus élevés.

05.2 INFORMATIONS

05.2.1 | RISQUES



- Exécution de code arbitraire (à distance)
- Élévation de privilèges

05.2.2 | CRITICITE

- **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**

05.2.3 | CVE

- CVE-2022-26931

05.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 ARM64-based Systems
- Microsoft Windows 10 20H2 x64-based Systems
- Microsoft Windows Server (Server Core installation) 2019
- Microsoft Windows Server (Server Core installation) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server (Server Core installation) 2012
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 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 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

05.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

05.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

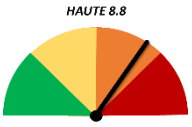
06 CVE-2022-26923 (AD)

06.1 RÉSUMÉ

Un défaut a été découvert dans Active Directory Domain Service (AD DS) du système d'exploitation Windows de Microsoft. Il est possible pour un attaquant distant et authentifié en tant que simple utilisateur d'utiliser une requête forgée afin d'exécuter de code arbitraire sur le système avec les privilèges les plus élevés.

06.2 INFORMATIONS

06.2.1 | RISQUES



- Exécution de code arbitraire (à distance)
- Élévation de privilèges

06.2.2 | CRITICITE

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

06.2.3 | CVE

- CVE-2022-26923

06.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- 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

06.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows server 2022: KB5013944

06.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

07 CVE-2022-26937 (NFS)

07.1 RÉSUMÉ

Identifiée dans le système de fichier NFS (Network File System) de Windows, la CVE-2022-26937 est une vulnérabilité critique qui peut être exploitée par un attaquant distant et non authentifiée.

Il est possible d'utiliser une requête forgée afin d'exécuter de code arbitraire sur le serveur ou sur le système d'exploitation.

07.2 INFORMATIONS

07.2.1 | RISQUES

- Exécution de code arbitraire (à distance)

07.2.2 | CRITICITE

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

07.2.3 | CVE

- CVE-2022-26937

07.2.4 | COMPOSANTS VULNERABLES.

- 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 (Server Core installation) 2008 R2
- 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

07.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.
- Une solution d'atténuation existe, celle-ci est détaillée ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 8.1, Windows server 2012: KB5014011 KB5014001
- Windows 10: KB5013952 KB5013941
- Windows server 2022: KB5013944
- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows server 2008: KB5014010 KB5014006

07.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment.

08 CVE-2022-22017 (RDC)

08.1 RÉSUMÉ

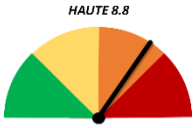
Cette vulnérabilité a été découverte dans le logiciel client Bureau à Distance du système d'exploitation Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et non authentifié d'exécuter du code arbitraire sur le système.

Pour réaliser son exploit, l'attaquant doit inciter l'utilisateur à ouvrir un fichier forgé : ce fichier force la connexion vers un serveur RDP malveillant à partir duquel l'offensive peut être réalisée.

08.2 INFORMATIONS

08.2.1 | RISQUES



- Exécution de code arbitraire (à distance)

08.2.2 | CRITICITE

- **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**

08.2.3 | CVE

- CVE-2022-22017

08.2.4 | COMPOSANTS VULNERABLES.

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

- Microsoft Windows 11 x64
- Microsoft Windows 11 ARM64
- Microsoft Remote Desktop Client Windows Desktop

08.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows server 2022: KB5013944
- Windows 11: KB5013943

08.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

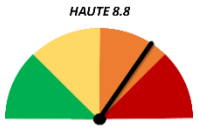
09 CVE-2022-30129 (VISUAL STUDIO CODE)

09.1 RÉSUMÉ

Cette vulnérabilité a été identifiée dans l'éditeur de code extensible Visual Studio Code. L'exploitation de cette vulnérabilité par un attaquant distant et non authentifié permet, en incitant un utilisateur à cliquer sur une URL forgée, d'exécuter du code arbitraire sur le système.

09.2 INFORMATIONS

09.2.1 | RISQUES



- Exécution de code arbitraire à distance

09.2.2 | CRITICITE

- **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**

09.2.3 | CVE

- CVE-2022-30129

09.2.4 | COMPOSANTS VULNERABLES.

- Microsoft Visual Studio Code

09.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.
- La dernière version de Visual Studio Code peut être téléchargée ici.

09.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

10 CVE-2022-21978 (EXCHANGE SERVER)

10.1 RÉSUMÉ

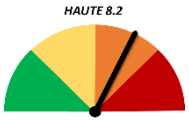
Les restrictions de sécurité ont été identifiées comme insuffisantes dans plusieurs produits Exchange Server de Microsoft.

L'exploitation de cette vulnérabilité par un attaquant local et authentifié permet une exécution de code arbitraire avec les privilèges les plus élevés.

10.2 INFORMATIONS

10.2.1 | RISQUES

- Élévation de privilèges
- Exécution de code arbitraire
- Contournement de la politique de sécurité



10.2.2 | CRITICITE

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

10.2.3 | CVE

- CVE-2022-21978

10.2.4 | COMPOSANTS VULNERABLES.

- Microsoft Exchange Server 2013 CU23
- Microsoft Exchange Server 2016 CU22
- Microsoft Exchange Server 2019 CU11
- Microsoft Exchange Server 2016 CU23
- Microsoft Exchange Server 2019 CU12

10.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Exchange Server 2019, 2016, 2013 : KB5014261 KB5014260

10.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

11 CVE-2022-23279 (ALPC)

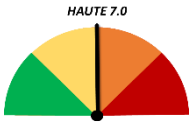
11.1 RÉSUMÉ

Identifiée dans le composant ALPC (Advanced Local Procedure Calls), la CVE-2022-23279 est une vulnérabilité de type « situation de concurrence (race condition) » qui affecte plusieurs produits Windows.

L'exploitation de cette vulnérabilité par un attaquant local et authentifié en tant que simple utilisateur permet, en utilisant un programme malveillant, d'exécuter de code arbitraire avec les privilèges les plus élevés.

11.2 INFORMATIONS

11.2.1 | RISQUES



- Élévation de privilèges
- Exécution de code arbitraire

11.2.2 | CRITICITE

- **La faille n'est pas activement exploitée,**
- **Vecteur d'attaque : Local**
- **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**

11.2.3 | CVE

- CVE-2022-23279

11.2.4 | COMPOSANTS VULNERABLES.

- Microsoft Windows 10 1909 32-bit Systems

- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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) 20H2
- 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

11.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 10: KB5013942 KB5013945
- Windows 11: KB5013943
- Windows server 2022: KB5013944

11.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

12 CVE-2022-22012 (LDAP)

12.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et non authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

12.2 INFORMATIONS

12.2.1 | RISQUES

- Exécution de code arbitraire

12.2.2 | CRITICITE

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

12.2.3 | CVE

- CVE-2022-22012

12.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 ARM64-based Systems
- Microsoft Windows 10 20H2 x64-based Systems
- Microsoft Windows Server (Server Core installation) 2019
- Microsoft Windows Server (Server Core installation) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server (Server Core installation) 2012
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 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 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

12.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

12.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

13 CVE-2022-22013 (LDAP)

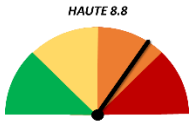
13.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

13.2 INFORMATIONS

13.2.1 | RISQUES



- Exécution de code arbitraire

13.2.2 | CRITICITE

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

13.2.3 | CVE

- CVE-2022-22013

13.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 ARM64-based Systems
- Microsoft Windows 10 20H2 x64-based Systems
- Microsoft Windows Server (Server Core installation) 2019
- Microsoft Windows Server (Server Core installation) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server (Server Core installation) 2012
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 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 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

13.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

13.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

14 CVE-2022-22014 (LDAP)

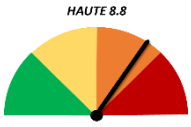
14.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

14.2 INFORMATIONS

14.2.1 | RISQUES



- Exécution de code arbitraire

14.2.2 | CRITICITE

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

14.2.3 | CVE

- CVE-2022-22014

14.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 ARM64-based Systems
- Microsoft Windows 10 20H2 x64-based Systems
- Microsoft Windows Server (Server Core installation) 2019
- Microsoft Windows Server (Server Core installation) 20H2
- Microsoft Windows Server (Server Core installation) 2016
- Microsoft Windows Server (Server Core installation) 2012 R2
- Microsoft Windows Server (Server Core installation) 2012
- Microsoft Windows Server X64-based systems (Server Core installation) 2008 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 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

14.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

14.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

15 CVE-2022-29128 (LDAP)

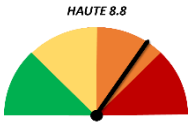
15.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

15.2 INFORMATIONS

15.2.1 | RISQUES



- Exécution de code arbitraire

15.2.2 | CRITICITE

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

15.2.3 | CVE

- CVE-2022-29128

15.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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 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

15.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

15.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

16 CVE-2022-29129 (LDAP)

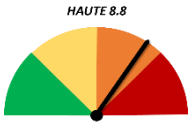
16.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

16.2 INFORMATIONS

16.2.1 | RISQUES



- Exécution de code arbitraire

16.2.2 | CRITICITE

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

16.2.3 | CVE

- CVE-2022-29129

16.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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 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

16.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

16.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

17 CVE-2022-29130 (LDAP)

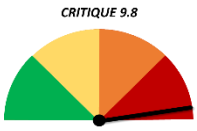
17.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et non authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

17.2 INFORMATIONS

17.2.1 | RISQUES



- Exécution de code arbitraire

17.2.2 | CRITICITE

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

17.2.3 | CVE

- CVE-2022-29130

17.2.4 | COMPOSANTS VULNERABLES.

- 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 for x64-based Systems
- Microsoft Windows 10 1809 for 32-bit Systems
- Microsoft Windows 10 1809 for ARM64-based Systems
- Microsoft Windows 10 1607 32-bit Systems
- Microsoft Windows 10 1607 x64-based Systems
- Microsoft Windows 10 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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 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

17.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5013999 KB5014018 KB5014012
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows server 2008: KB5014010 KB5014006
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

17.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

18 CVE-2022-29131 (LDAP)

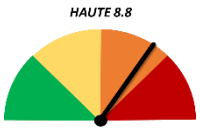
18.1 RÉSUMÉ

Une vulnérabilité a été identifiée dans une composante du protocole LDAP, celle-ci affecte différents systèmes d'exploitation et serveurs Windows de Microsoft.

L'exploitation de cette vulnérabilité peut permettre à un attaquant distant et authentifié, en utilisant une requête forgée, d'exécuter du code arbitraire sur le système.

18.2 INFORMATIONS

18.2.1 | RISQUES



- Exécution de code arbitraire

18.2.2 | CRITICITE

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

18.2.3 | CVE

- CVE-2022-29131

18.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-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 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

18.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 10: KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

18.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

19 CVE-2022-29104 (PRINT SPOOLER)

19.1 RÉSUMÉ

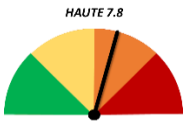
La CVE-2022-29104 est une vulnérabilité qui a été identifiée dans le service de spooling dédiée à la gestion des tâches d'impression du système d'exploitation Windows.

La vulnérabilité existe en raison d'une insuffisance des restrictions de sécurité. L'exploitation de cette vulnérabilité par un attaquant local et authentifié peut permettre, en utilisant un programme malveillant, d'exécuter du code arbitraire sur le système avec les privilèges les plus élevés.

19.2 INFORMATIONS

19.2.1 | RISQUES

- Élévation de privilèges
- Exécution de code arbitraire
- Contournement e la politique de sécurité



19.2.2 | CRITICITE

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

19.2.3 | CVE

- CVE-2022-29104

19.2.4 | COMPOSANTS VULNERABLES.

- 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 1909 32-bit Systems
- Microsoft Windows 10 1909 x64-based Systems
- Microsoft Windows 10 1909 ARM64-based Systems
- Microsoft Windows 10 20H2 32-bit Systems
- Microsoft Windows 10 20H2 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 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 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

19.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows 7: KB5014018
- Windows 8, Windows server 2012: KB5014017
- Windows 8.1, Windows server 2012: KB5014011 KB5014001 KB5014025
- Windows 10: KB5013952 KB5013963 KB5013942 KB5013945 KB5013941
- Windows 11: KB5013943
- Windows server 2022: KB5013944

19.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

20 CVE-2022-29109 (EXCEL)

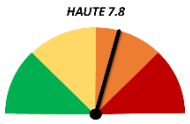
20.1 RÉSUMÉ

Cette vulnérabilité concerne le logiciel tableur Excel de Windows. En incitant un utilisateur à ouvrir un fichier forgé, un attaquant local et non authentifié peut faire exécuter du code arbitraire sur le système.

Dans le bulletin CVE-2022-29109 publié par Microsoft le 10 mai 2022, le vecteur d'attaque est précisé comme étant **local**. Selon l'expertise de cybersecurity-help, le vecteur d'attaque serait aussi **réseau**, ce qui signifie que l'attaque pourrait être réalisée localement ou à distance.

20.2 INFORMATIONS

20.2.1 | RISQUES



- Exécution de code arbitraire

20.2.2 | CRITICITE

- **La faille n'est pas activement exploitée,**
- **Vecteur d'attaque : Local (Selon Microsoft)**
- **Vecteur d'attaque : Réseau (Selon Cybersecurity-Help)**
- **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**

20.2.3 | CVE

- CVE-2022-29109

20.2.4 | COMPOSANTS VULNERABLES.

- Microsoft Office Online Server

- Microsoft Office 2019 Click-to-Run x32
- Microsoft Office 2019 Click-to-Run x64
- Microsoft 365 Apps for Enterprise x32
- Microsoft 365 Apps for Enterprise x64
- Microsoft Office LTSC 2021 x32
- Microsoft Office LTSC 2021 x64

20.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows Office Online Server: KB5002205

20.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

21 CVE-2022-29110 (EXCEL)

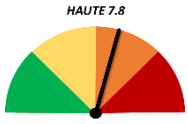
21.1 RÉSUMÉ

Cette vulnérabilité concerne le logiciel tableur Excel de Windows. En incitant un utilisateur à ouvrir un fichier forgé, un attaquant local et non authentifié peut faire exécuter du code arbitraire sur le système.

Dans le bulletin CVE-2022-29110 publié par Microsoft le 10 mai 2022, le vecteur d'attaque est précisé comme étant **local**. Selon l'expertise de cybersecurity-help, le vecteur d'attaque serait aussi par **réseau**, ce qui signifie que l'attaque pourrait être réalisée localement ou à distance.

21.2 INFORMATIONS

21.2.1 | RISQUES



- Exécution de code arbitraire

21.2.2 | CRITICITE

- **La faille n'est pas activement exploitée,**
- **Vecteur d'attaque : Local (Selon Microsoft)**
- **Vecteur d'attaque : Réseau (Selon Cybersecurity-Help)**
- **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**

21.2.3 | CVE

- CVE-2022-29110

21.2.4 | COMPOSANTS VULNERABLES.

- Microsoft Excel 2013 SP1 RT

- Microsoft Excel 2016 x32
- Microsoft Excel 2016 x64
- Microsoft Office Web Apps Server 2013 SP1
- Microsoft Excel 2013 SP1 32-bit edition
- Microsoft Excel 2013 SP1 64-bit edition

21.3 RECOMMANDATIONS

- Une mise à jour de Microsoft (Patch Tuesday mai 2022) permet d'apporter le correctif nécessaire.
- Des informations supplémentaires sont disponibles ici.

Les mises à jour de sécurité cumulatives, datées du 10 mai 2022, pour les produits concernés par la vulnérabilité sont ci-dessous.

- Windows Office Web Apps Server 2013: KB5002199
- Microsoft Office 2013 Service, Excel: KB5002204
- Excel 2016: KB5002196

21.4 PROOF OF CONCEPT

Aucun exploit (POC) n'est disponible pour le moment

22 REFERENCES

https://www.ginjfo.com/actualites/securite-informatique/windows-10-et-11-le-patch-tuesday-de-mai-2022-debute-tous-les-details-20220511

https://www.lemondeinformatique.fr/actualites/lire-patch-tuesday-mai-2022-74-failles-corrigees-dont-1-exploitee-86733.html

https://www.monwindows.com/blog/kb5013943-pour-windows-11-la-mise-a-jour-de-mai-est-disponible-t114058.html

https://nvd.nist.gov/vuln/detail/CVE-2022-21972

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21972

https://nvd.nist.gov/vuln/detail/CVE-2022-23270

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23270

https://nvd.nist.gov/vuln/detail/CVE-2022-26931

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26931

https://nvd.nist.gov/vuln/detail/CVE-2022-26923

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923

https://nvd.nist.gov/vuln/detail/CVE-2022-26937

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937

https://nvd.nist.gov/vuln/detail/CVE-2022-22017

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017

https://nvd.nist.gov/vuln/detail/CVE-2022-26925

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26925

https://nvd.nist.gov/vuln/detail/CVE-2022-30129

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30129

https://nvd.nist.gov/vuln/detail/CVE-2022-21978

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978

https://nvd.nist.gov/vuln/detail/CVE-2022-23279

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23279

https://nvd.nist.gov/vuln/detail/CVE-2022-22012

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22012

https://nvd.nist.gov/vuln/detail/CVE-2022-22013

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22013

https://nvd.nist.gov/vuln/detail/CVE-2022-22014

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22014

https://nvd.nist.gov/vuln/detail/CVE-2022-29104

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29104

https://nvd.nist.gov/vuln/detail/CVE-2022-29109

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29109

https://nvd.nist.gov/vuln/detail/CVE-2022-29110

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110

https://nvd.nist.gov/vuln/detail/CVE-2022-29128

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29128

https://nvd.nist.gov/vuln/detail/CVE-2022-29129

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29129

https://nvd.nist.gov/vuln/detail/CVE-2022-29130

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29130

https://nvd.nist.gov/vuln/detail/CVE-2022-29131

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29131

advens
CYBERSECURITY

advens.fr

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