aDvens

Security for the greater good

Bulletin de vulnérabilités

Patch Tuesday du mois de janvier 2025

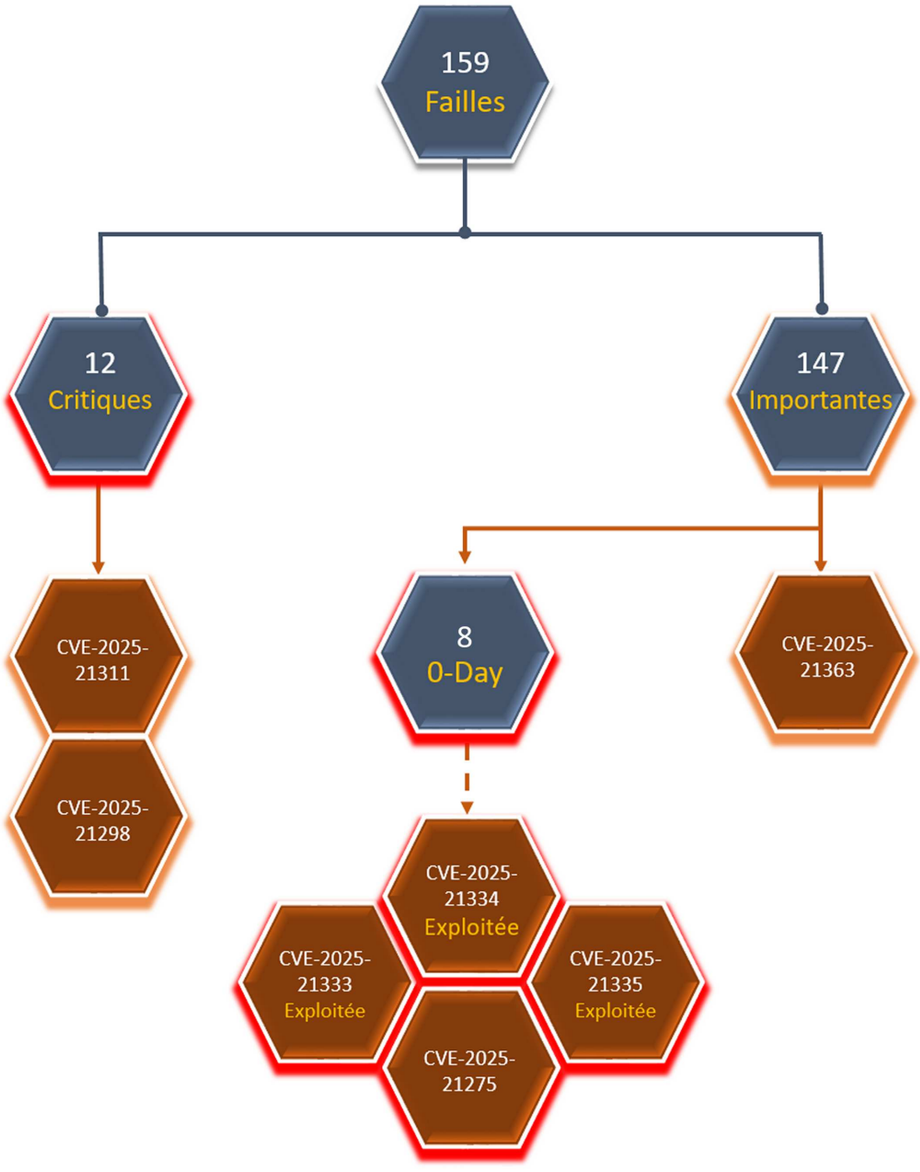
2025-01-15 |
CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

SOMMAIRE

SYNTHÈSE

Le mardi 14 janvier 2025, Microsoft a publié son bulletin mensuel ***Patch tuesday***, avec **159 failles** corrigées dont **3 exploitées** : CVE-2025-21333,CVE-2025-21334,CVE-2025-21335.

Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.



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

PRODUIT	CVE	SCORE	EPSS	ZERO-DAY	EXPLOITEE	CWE	POC
Windows Hyper V	CVE-2025-21333	7.8	0.14%	Oui	Oui	122	Non
Windows Hyper V	CVE-2025-21334	7.8	0.14%	Oui	Oui	416	Non
Windows Hyper V	CVE-2025-21335	7.8	0.14%	Oui	Oui	416	Non
Windows App Package Installer	CVE-2025-21275	7.8	En cours	Oui	Non	285	Non
Windows NTLM	CVE-2025-21311	9.8	0.09%	Non	Non	303	Non
Windows OLE	CVE-2025-21298	8.8	0.09%	Non	Non	416	Non
Windows Word	CVE-2025-21363	7.8	0.05%	Non	Non	822	Non

HYPER-V - CVE-2025-21333, CVE-2025-21334 & CVE-2025-21335

Ces vulnérabilités exploitées affectent *Windows Hyper-V NT Kernel Integration VSP*. Elles permettent à un attaquant authentifié d'exécuter du code arbitraire avec les privilèges *SYSTEM*.

Aucune information technique concernant ces vulnérabilités n'est disponible actuellement, cependant le score semble indiquer que l'exploitation s'effectue depuis la machine hôte et pas depuis la machine virtuelle.

Ces vulnérabilités sont exploitées.

Type de vulnérabilité

Pour la CVE-2025-21333 :

- **CWE-122** : Heap-based Buffer Overflow

Pour les CVE-2025-21334 et CVE-2025-21335 :

- **CWE-416** : Use After Free

Risque

- Élévation de privilèges

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Windows 10
- Windows 11
- Windows Server 2022
- Windows Server 2025

Recommandations

KB5050009

- Windows Server 2025
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows Server 2025 (Server Core installation)

KB5049984

- Windows Server 2022, 23H2 Edition (Server Core installation)

KB5050021

- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5049981

- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems

Des informations complémentaires sont disponibles dans les bulletins CVE-2025-21333, CVE-2025-21334 et CVE-2025-21335 de Microsoft.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

WINDOWS APP PACKAGE INSTALLER - CVE-2025-21275

La CVE-2025-21275 est une vulnérabilité zero-day qui affecte le programme d'installation d'application de Windows.

Un défaut de contrôle des autorisations permet à un attaquant local et authentifié d'élever ses privilèges.

Type de vulnérabilité

- **CWE-285** : Improper Authorisation

Risque

- Élévation de privilèges

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Windows 10
- Windows 11
- Windows Server 2022
- Windows Server 2025

Recommandations

KB5050009

- Windows Server 2025
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows Server 2025 (Server Core installation)

KB5049984

- Windows Server 2022, 23H2 Edition (Server Core installation)

KB5050021

- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5049981

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

KB5049983

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

Des informations complémentaires sont disponibles dans le Bulletin de Microsoft.

Preuve de concept

Aucune preuve de concept n'est disponible en sources ouvertes.

WINDOWS NTLM - CVE-2025-21311

La CVE-2025-21311 est une vulnérabilité critique qui affecte le protocole Windows NTLM.

Les chercheurs en sécurité ont identifié une implémentation incorrecte de l'algorithme d'authentification.

L'exploitation de cette vulnérabilité permet à un attaquant distant d'obtenir des privilèges élevés sur le système.

Type de vulnérabilité

- **CWE-303** : Incorrect Implementation of Authentication Algorithm

Risque

- Élévation de privilèges

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Windows 11
- Windows Server 2022
- Windows Server 2025

Recommandations

KB5050009

- Windows Server 2025
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows Server 2025 (Server Core installation)

KB5049984

- Windows Server 2022, 23H2 Edition (Server Core installation)

Des informations complémentaires sont disponibles dans le bulletin de Microsoft

Pour limiter le risque d'exploitation, Microsoft recommande de configurer sur tous les systèmes le paramètre *LmCompatibilityLvl* à sa valeur maximale (5). Cette configuration empêche l'utilisation de l'ancien protocole NTLMv1, tout en autorisant NTLMv2. De plus, Microsoft recommande la lecture la documentation Network security: LAN Manager authentication level.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

MICROSOFT OLE - CVE-2025-21298

Cette vulnérabilité, découverte par des chercheurs en sécurité de Zero Day Initiative, affecte Windows OLE.

Le problème est due à un défaut de traitement de fichiers RTF et permet à un attaquant d'exécuter du code arbitraire via des emails spécifiquement forgés. Le mode de "prévisualisation" d'Outlook n'étant pas vulnérable, l'attaquant doit persuader la victime d'ouvrir l'email, de prévisualiser une pièce jointe spécifiquement forgée ou de consulter un document malveillant avec Microsoft Word.

Une interaction utilisateur semble nécessaire à cette exploitation. Par conséquent le CERT aDvens a modifié le score CVSS (3.1) de 9.8 a 8.8.

Type de vulnérabilité

- **CWE-416** : Use After Free

Risque

- Exécution de code à distance

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Windows 10
- Windows 11
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Recommandations

KB5050048

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

KB5050004

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

KB5050049

- 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

KB5050006

- 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

KB5050063

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

KB5050061

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

KB5049993

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

KB5050013

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

KB5050009

- Windows Server 2025
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows Server 2025 (Server Core installation)

KB5049984

- Windows Server 2022, 23H2 Edition (Server Core installation)

KB5050021

- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5049981

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

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

KB5049983

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

KB5050008

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

Si les correctifs ne peuvent pas être appliqués, Microsoft recommande de consulter les emails en texte brut en suivant la procédure décrite ici.

Des informations complémentaires sont disponibles dans les bulletins de Microsoft et de Zero Day Initiative.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

MICROSOFT WORD - CVE-2025-21363

Découverte par les équipes de sécurité de Zero Day Initiative, cette vulnérabilité affecte Microsoft Word.

Un défaut de libération de pointeur dans Microsoft Word permet à un attaquant d'exécuter du code arbitraire sur le système en persuadant la victime d'ouvrir un fichier DOCX spécifiquement forgé.

Type de vulnérabilité

- **CWE-822** : Untrusted Pointer Dereference

Risque

- Exécution de code à distance

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Microsoft Office LTSC for Mac 2024
- Microsoft Office LTSC 2024 for 64-bit editions
- Microsoft Office LTSC 2024 for 32-bit editions
- Microsoft Office LTSC for Mac 2021
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems

Recommandations

Correctif Mac

- Microsoft Office LTSC for Mac 2024
- Microsoft Office LTSC for Mac 2021

Correctif Office

- Microsoft Office LTSC 2024 for 64-bit editions
- Microsoft Office LTSC 2024 for 32-bit editions

- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems

Des informations complémentaires sont disponibles dans les bulletins de Microsoft et de Zero Day Initiative.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

RÉFÉRENCES

Articles

- https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2025-patch-tuesday-fixes-8-zero-days-159-flaws/
- https://www.zerodayinitiative.com/blog/2025/1/14/the-january-2025-security-update-review

HYPER V - CVE-2025-21333

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21333
- https://nvd.nist.gov/vuln/detail/CVE-2025-21333
- https://www.cybersecurity-help.cz/vdb/SB2025011444
- https://www.cve.org/CVERecord?id=CVE-2025-21333

HYPER V - CVE-2025-21334

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21334
- https://nvd.nist.gov/vuln/detail/CVE-2025-21334
- https://www.cybersecurity-help.cz/vdb/SB2025011444
- https://www.cve.org/CVERecord?id=CVE-2025-21334

HYPER V - CVE-2025-21335

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21335
- https://nvd.nist.gov/vuln/detail/CVE-2025-21335
- https://www.cybersecurity-help.cz/vdb/SB2025011444
- https://www.cve.org/CVERecord?id=CVE-2025-21335

Windows App Package Installer - CVE-2025-21275

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21275
- https://nvd.nist.gov/vuln/detail/CVE-2025-21275
- https://www.cybersecurity-help.cz/vdb/SB2025011507
- https://www.cve.org/CVERecord?id=CVE-2025-21275

Windows NTLM - CVE-2025-21311

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21311
- https://nvd.nist.gov/vuln/detail/CVE-2025-21311
- https://www.cybersecurity-help.cz/vdb/SB2025011524
- https://www.cve.org/CVERecord?id=CVE-2025-21311

Windows OLE - CVE-2025-21298

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21298
- https://nvd.nist.gov/vuln/detail/CVE-2025-21298
- https://www.cybersecurity-help.cz/vdb/SB2025011538
- https://www.cve.org/CVERecord?id=CVE-2025-21298
- https://www.zerodayinitiative.com/advisories/ZDI-25-028/

Microsoft Word - CVE-2025-21363

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-21363
- https://nvd.nist.gov/vuln/detail/CVE-2025-21363

- https://www.cybersecurity-help.cz/vdb/SB2025011520
- https://www.cve.org/CVERecord?id=CVE-2025-21363
- https://www.zerodayinitiative.com/advisories/ZDI-25-028/