

CSIRT · RAPPORT D'ANALYSE · UNIDEES-CSIRT-141026-001

Patch Tuesday d'octobre 2026 : analyse des 1 407 correctifs et priorités de déploiement

Analyse du CSIRT UNIDEES, publiée le 23/10/2026 : failles exploitées,
probabilités d'exploitation et ordre de déploiement recommandé.

Synthèse pour la direction

- Microsoft a corrigé **1 407 vulnérabilités** le 13 octobre 2026, dont **77 critiques**. Près d'une sur deux (674) est une élévation de privilèges : elle ne sert pas à entrer dans un système, mais à en prendre le contrôle une fois entré.
- **Une seule faille était exploitée** : CVE-2026-96951 (Windows Shell), qui supprime l'avertissement affiché à l'ouverture d'un fichier venu d'Internet. Notée 8,8, elle n'est pas « critique » sur le papier, mais c'est la priorité absolue.
- **Au 23/10/2026, aucune autre n'est signalée exploitée** (catalogue CISA du 21/10/2026) et la probabilité d'exploitation mesurée (EPSS) ne dépasse pas 2,9 %. Ce délai est à mettre à profit pour déployer.
- **54 failles permettent d'exécuter du code à distance sans compte ni action de l'utilisateur** (Outlook, DHCP, DNS, QUIC, Message Queuing, RRAS...). Ce sont les plus faciles à exploiter à grande échelle.
- **La gravité affichée par Microsoft ne suffit pas** : 61 failles ont un score CVSS de 9 ou plus, dont 47 classées seulement « importantes ».
- **Plusieurs produits encore répandus ne reçoivent plus de correctifs** depuis ce mois-ci (Windows Server 2012 et 2012 R2, Office 2021, Windows 11 24H2 Famille et Professionnel...).

Décisions recommandées

1. Déployer sans attendre le correctif de CVE-2026-96951 sur tous les postes et serveurs Windows.
2. Sous 72 heures, les serveurs exposés (Exchange, AD FS, RRAS, services publiés sur Internet) ; sous sept jours, le cœur de l'infrastructure (contrôleurs de domaine, DHCP, DNS, SharePoint) et Office et Outlook sur tous les postes.
3. Recenser les produits arrivés en fin de support et décider, pour chacun, de leur remplacement ou de leur isolement.

Les chiffres du mois

1 407

vulnérabilités corrigées

77

critiques selon Microsoft

1

exploitée avant le correctif

2

divulguées publiquement (dont 1 hors Microsoft)

314

exécutions de code à distance

54

exécutions de code sans compte ni action

Calculs du CSIRT sur les données officielles de Microsoft (mises à jour au 22/10/2026) : CVE publiées par Microsoft le 13/10/2026. Nous retenons les chiffres de la source officielle à la date des données.

PAR TYPE D'IMPACT

Élévation de privilèges		674
Exécution de code à distance		314
Divulgarion d'informations		252
Déni de service		71
Contournement de sécurité		40
Falsification		29
Usurpation		27

COMPOSANTS LES PLUS TOUCHÉS

Microsoft Office Excel		69
Role: DNS Server		52
Windows Kernel		46
Windows Installer		38
Windows Win32 Kernel Subsystem		36
Microsoft Office SharePoint		36
Microsoft Windows Search Component		29
Windows NTFS		26
.NET		25
Microsoft Office Word		22

Le volume est inhabituel, mais il ne change pas la méthode : l'essentiel du risque se concentre sur une poignée de failles exploitées, exposées sur le réseau ou jugées « plus probables » par Microsoft (108 ce mois-ci). Ce sont elles qu'il faut traiter en premier ; le reste suit le cycle normal de mise à jour.

Ce qui est exploité, et ce qui risque de l'être

Au 21/10/2026, le catalogue CISA des vulnérabilités exploitées ne contient qu'une faille de ce Patch Tuesday : **CVE-2026-96951**, ajoutée le 13/10/2026. Deux failles avaient été rendues publiques avant le correctif : CVE-2026-108398 (.NET Framework, contournement de WDAC) et CVE-2026-92707 (bibliothèque MessagePack-CSharp, déni de service, gravité « modérée », attribuée par GitHub et donc hors du périmètre ci-dessus). Le score EPSS, qui estime la probabilité d'une exploitation dans les 30 jours, reste bas pour toutes les autres : le plus élevé est de 2,9 % (CVE-2026-88091). Voici les dix plus fortes probabilités mesurées.

CVE	COMPOSANT	IMPACT	GRAVITÉ	CVSS	EPSS
CVE-2026-88091	Windows Management Instrumentation	Élévation de privilèges	Importante	7,8	2,9 %
CVE-2026-70049	Microsoft Configuration Manager	Élévation de privilèges	Importante	8,0	2,3 %
CVE-2026-96186	Microsoft Windows Media Foundation	Élévation de privilèges	Importante	7,8	2,3 %
CVE-2026-100214	Dynamics Business Central	Exécution de code à distance	Importante	8,8	1,8 %
CVE-2026-87692	Microsoft Exchange Server	Élévation de privilèges	Importante	7,8	1,6 %
CVE-2026-85900	Microsoft Office SharePoint	Exécution de code à distance	Importante	8,8	1,5 %
CVE-2026-96951	Windows Shell	Contournement de sécurité	Importante	8,8	1,5 %
CVE-2026-70035	.NET Framework	Exécution de code à distance	Importante	8,8	1,3 %
CVE-2026-83520	.NET	Exécution de code à distance	Importante	8,8	1,3 %
CVE-2026-70058	Windows DHCP Server	Exécution de code à distance	Importante	7,5	1,2 %

EPSS du 22/10/2026 (FIRST). Un score bas n'est pas une garantie : il évolue dès qu'un code d'exploitation circule.

Les priorités du CSIRT

Classement par risque réel, et non par score seul : exploitation avérée, divulgation publique, exposition réseau sans authentification, appréciation de Microsoft (« exploitation plus probable ») et probabilité mesurée (EPSS).

-
- 01 Windows Shell : contournement de « Mark of the Web », exploité**
CVE-2026-96951 (importante, CVSS 8,8)
Seule faille du mois exploitée avant le correctif. Elle supprime l'avertissement affiché à l'ouverture d'un fichier venu d'Internet : un attaquant n'a plus qu'à convaincre la victime d'ouvrir une pièce jointe. Inscrite au catalogue CISA le 13/10.
-
- 02 .NET Framework : contournement de WDAC, divulgué publiquement**
CVE-2026-108398 (importante, CVSS 8,8)
Détails publiés avant le correctif. Permet de contourner le contrôle des applications (WDAC) en faisant charger un assemblage .NET malveillant par un processus protégé.
-
- 03 Outlook : cinq exécutions de code à distance critiques**
CVE-2026-70291 (critique, CVSS 9,8) · CVE-2026-70242 (critique, CVSS 9,8) · CVE-2026-97016 (critique, CVSS 9,8) · CVE-2026-88156 (critique, CVSS 9,8) · CVE-2026-97749 (critique, CVSS 9,8)
Score 9,8, sans authentification ni action de l'utilisateur selon le vecteur publié. Outlook est présent sur la quasi-totalité des postes.
-
- 04 Exchange Server : exécution de code, usurpation et élévation de privilèges**
CVE-2026-70571 (critique, CVSS 8,1) · CVE-2026-70279 (importante, CVSS 9,3) · CVE-2026-87692 (importante, CVSS 7,8)
Microsoft juge l'exploitation « plus probable » pour les deux premières, la première étant critique et atteignable sans authentification. Un serveur Exchange est exposé par nature et reste une cible prioritaire des attaquants.
-
- 05 Active Directory Domain Services : exécution de code critique**
CVE-2026-70229 (critique, CVSS 8,1)
Un paquet réseau forgé suffit, et l'exploitation est jugée « plus probable ». Compromettre un contrôleur de domaine, c'est compromettre tout le système d'information.
-
- 06 Serveur DHCP Windows : exécution de code critique**
CVE-2026-96934 (critique, CVSS 9,8)
Score 9,8, accessible par le réseau sans authentification. Les serveurs DHCP sont présents dans presque toutes les infrastructures.
-
- 07 Microsoft QUIC : deux exécutions de code critiques**
CVE-2026-105016 (critique, CVSS 9,8) · CVE-2026-100219 (critique, CVSS 9,8)
Score 9,8 sans authentification. QUIC est utilisé par HTTP/3 et par SMB sur QUIC : à traiter en priorité sur les serveurs publiés sur Internet.
-
- 08 Message Queuing : exécution de code critique**
CVE-2026-100202 (critique, CVSS 9,8)
Score 9,8 sans authentification. Vérifier si le service MSMQ est activé : il l'est souvent sans être utilisé.
-
- 09 Word, PowerPoint, rendu des polices et pilote PostScript**
CVE-2026-70300 (critique, CVSS 9,8) · CVE-2026-88178 (critique, CVSS 9,8) · CVE-2026-97814 (critique, CVSS 9,8) · CVE-2026-70147 (critique, CVSS 9,8) · CVE-2026-70153 (critique, CVSS 9,8)
Exécutions de code critiques, notées 9,8, dans le traitement des documents, des polices et de l'impression. Avec la faille Windows Shell exploitée, les fichiers piégés restent le vecteur d'attaque à surveiller ce mois-ci.
-
- 10 SharePoint : exécution de code à distance**
CVE-2026-85900 (importante, CVSS 8,8)
Parmi les plus fortes probabilités d'exploitation mesurées (EPSS) ce mois-ci. SharePoint concentre souvent des documents sensibles.

- 11 Dynamics 365 Business Central, WebDAV et BITS**
 CVE-2026-100214 (importante, CVSS 8,8) · CVE-2026-102217 (importante, CVSS 8,8) · CVE-2026-88159 (importante, CVSS 8,8)
 Exploitation jugée « plus probable » par Microsoft ; Business Central a la plus forte probabilité d'exploitation (EPSS) des exécutions de code du mois.
- 12 Élévations de privilèges : WMI, Media Foundation, Configuration Manager**
 CVE-2026-88091 (importante, CVSS 7,8) · CVE-2026-96186 (importante, CVSS 7,8) · CVE-2026-70049 (importante, CVSS 8,0)
 Les trois plus fortes probabilités d'exploitation (EPSS) du mois ; pour Configuration Manager, Microsoft indique qu'un code d'exploitation de démonstration existe. Une élévation de privilèges transforme un poste compromis en prise de contrôle complète.

Lecture par environnement

ENVIRONNEMENT	FAILLES	CRITIQUES	EXÉC. CODE	PLUS PROBABLES
Active Directory et identité Contrôleurs de domaine et AD FS d'abord : une seule compromission suffit à prendre tout le domaine.	39	3	4	2
Exchange Server Serveurs exposés par nature : à mettre à jour dans les 72 heures.	9	1	1	2
SharePoint Volume élevé de correctifs ce mois-ci ; priorité aux fermes publiées sur Internet.	36	1	7	0
Office et Outlook Le plus grand nombre de failles critiques : déployer sur tous les postes par l'outil de gestion habituel.	191	35	111	0
Services réseau (DNS, DHCP, RRAS, RDP, IIS, SMB, QUIC...) Les failles atteignables sans compte se trouvent surtout ici : commencer par les serveurs exposés.	172	11	65	2
SQL Server Aucune faille critique, mais des exécutions de code : à intégrer à la fenêtre de maintenance du mois.	23	0	9	0
.NET et Visual Studio Inclut la faille divulguée publiquement ; penser aux serveurs d'applications et aux postes de développement.	56	0	16	0
Hyper-V et virtualisation Une faille sur l'hyperviseur touche toutes les machines virtuelles qu'il héberge.	18	3	4	0
Noyau et pilotes Windows Surtout des élévations de privilèges, souvent jugées « plus probables » : elles servent à la seconde étape d'une attaque.	299	7	22	34

Fins de support à ne pas manquer

- Windows Server 2012 et 2012 R2 : dernière année des mises à jour de sécurité étendues (ESU) terminée le 13/10/2026.
- Windows 10 Entreprise LTSB 2016 et IoT Entreprise LTSB 2016 : fin du support étendu.
- Office 2021, Office LTSC 2021 (Windows et Mac) et Skype Entreprise LTSC 2021 : fin du support.

- Windows 11 version 24H2 Famille et Professionnel : dernière mise à jour de sécurité.
- Windows Server 2022 : fin du support standard ; le support étendu se poursuit jusqu'au 14/10/2031.

Plan de déploiement recommandé

Sous 72 h

Faible exploitée et serveurs exposés

CVE-2026-96951 partout ; Exchange, AD FS, RRAS, serveurs publiant QUIC ou IIS sur Internet.

Sous 7 jours

Cœur de l'infrastructure et postes

Contrôleurs de domaine, DHCP, DNS, SharePoint, Hyper-V ; Office et Outlook sur tous les postes.

Sous 30 jours

Le reste du parc

Serveurs internes, SQL Server, .NET, postes de développement ; puis contrôle de conformité des mises à jour par un scan de vulnérabilités.

Besoin d'aide pour prioriser ou vérifier vos déploiements ?

Le CSIRT d'UNIDEES accompagne les organisations : priorisation adaptée à votre parc, suivi du déploiement, scan de vérification et recherche de traces de compromission. Le CSIRT et le SOC managé d'UNIDEES sont certifiés ISO/IEC 27001:2022. Contact : commercial@unidees.dz

Méthode et limites

Périmètre : les CVE dont Microsoft est l'autorité d'attribution et qui ont été publiées le 13/10/2026, soit 1 407, lues dans les données officielles de Microsoft (CVRF) mises à jour au 22/10/2026. Gravité : la plus élevée attribuée par Microsoft parmi les produits concernés. Exploitation : catalogue CISA KEV (version 21/10/2026) et indicateurs de Microsoft. Probabilité : EPSS du 22/10/2026. Les décomptes par gravité et par composant portent sur les données au 22/10/2026. Les fins de support sont vérifiées sur le site officiel du cycle de vie de Microsoft. La situation évolue : ce rapport décrit l'état au 23/10/2026.

Sources

- Microsoft MSRC · notes de version d'octobre 2026 / October 2026 release notes
<https://msrc.microsoft.com/update-guide/releaseNote/2026-Oct>
- Microsoft MSRC · données CVRF / CVRF data
<https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Oct>
- CISA · Known Exploited Vulnerabilities
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- FIRST · EPSS
<https://www.first.org/epss/>
- Microsoft · fins de support 2026 / 2026 end of support
<https://learn.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2026>