TLP:CLEAR

CSIRT · RAPPORT D'ANALYSE · UNIDEES-CSIRT-111126-001

Patch Tuesday de novembre 2026 : analyse des 1 093 correctifs et priorités de déploiement

Analyse du CSIRT UNIDEES, publiée le 11/11/2026 : faille exploitée, exposition réseau et ordre de déploiement recommandé.

PUBLICATION	VERSION	CLASSIFICATION	DONNÉES
11/11/2026	v1.0	Public	Microsoft au 10/11/2026

Synthèse pour la direction

- Microsoft a corrigé **1 093 vulnérabilités** le 10 novembre 2026, dont **63 critiques**. Près d'une sur deux (534) 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-2026-124194 (Outlook), une usurpation classée seulement « modérée » par Microsoft (CVSS 6,5). La CISA l'a inscrite à son catalogue des failles exploitées le 10/11/2026 : c'est la priorité absolue.
- **Aucune faille n'a été divulguée publiquement avant le correctif**, et aucune autre n'est signalée exploitée au 10/11/2026 (catalogue CISA).
- **Les probabilités d'exploitation (EPSS) ne sont pas encore disponibles** : au 10/11/2026, aucun score n'était publié pour ces failles, apparues le jour même. Cette absence ne signifie pas un risque faible ; ce mois-ci, nos priorités reposent sur l'exploitation avérée, l'exposition réseau et l'appréciation de Microsoft (42 failles jugées « exploitation plus probable »).
- **12 failles permettent d'exécuter du code à distance sans compte, sans action de l'utilisateur et avec une faible complexité d'attaque** (LDAP, Windows Search, DNS, DHCP, iSCSI, SQL Server…) : ce sont les plus faciles à exploiter à grande échelle. 21 autres le permettent aussi, mais dans des conditions plus difficiles à réunir (complexité d'attaque élevée), notamment Message Queuing, Schannel et NAT.
- **La gravité affichée par Microsoft ne suffit pas** : 23 failles ont un score CVSS de 9 ou plus, dont 19 classées seulement « importantes » (notamment DNS, DHCP, Kerberos et SQL Server).
- **Plusieurs produits arrivent en fin de support le 10/11/2026** : .NET 8, PowerShell 7.4 et Windows 11 Entreprise et Éducation, version 23H2.

Décisions recommandées

1. Déployer sans attendre le correctif de CVE-2026-124194 sur tous les postes équipés d'Outlook (Microsoft 365 Apps, Office LTSC 2021 et 2024).
2. Sous 72 heures, les contrôleurs de domaine, Exchange et les serveurs exposés (DNS, DHCP, services publiés sur Internet) ; sous sept jours, Office sur tous les postes, SQL Server, SharePoint et Hyper-V.
3. Recenser les environnements .NET 8, PowerShell 7.4 et Windows 11 23H2 arrivés en fin de support, et décider de leur migration.

Les chiffres du mois

1 093
vulnérabilités corrigées

63
critiques selon Microsoft

1
exploitée avant le correctif

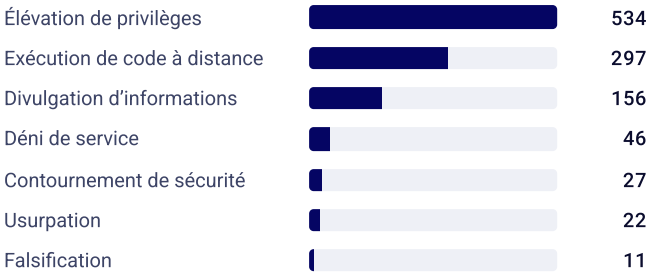
0
divulguée publiquement avant le correctif

297
exécutions de code à distance

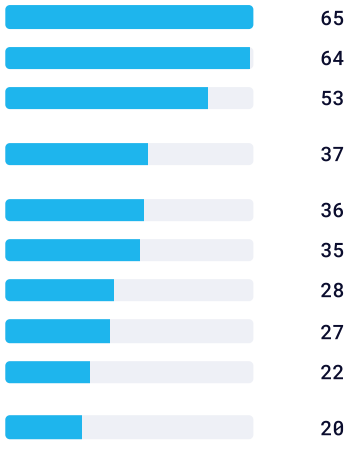
12
exécutions de code sans compte ni action, faible complexité

Calculs du CSIRT sur les données officielles de Microsoft (mises à jour au 10/11/2026) : CVE publiées par Microsoft le 10/11/2026. Nous retenons les chiffres de la source officielle à la date des données.

PAR TYPE D'IMPACT



COMPOSANTS LES PLUS TOUCHÉS



Le volume reste très élevé, mais l'essentiel du risque se concentre sur une poignée de failles : celle qui est exploitée, celles atteignables par le réseau sans compte, et celles que Microsoft juge « exploitation plus probable » (42 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 10/11/2026, le catalogue CISA des vulnérabilités exploitées ne contient qu'une faille de ce Patch Tuesday : **CVE-2026-124194** (Outlook, usurpation), ajoutée le 10/11/2026 ; Microsoft la signale également comme exploitée. Aucune faille n'avait été rendue publique avant le correctif. **Les scores EPSS ne sont pas encore publiés** pour ces failles, apparues le jour même : nous ne tirons donc aucune conclusion de la probabilité d'exploitation mesurée. Le tableau présente la faille exploitée, puis celles que Microsoft juge « exploitation plus probable », les critiques d'abord, par score CVSS décroissant.

CVE	COMPOSANT	IMPACT	GRAVITÉ	CVSS	EPSS
CVE-2026-124194	Microsoft Office Outlook	Usurpation	Modérée	6,5	n.d.
CVE-2026-118146	Active Directory Domain Services	Exécution de code à distance	Critique	8,8	n.d.
CVE-2026-118207	Microsoft Exchange Server	Exécution de code à distance	Critique	8,8	n.d.
CVE-2026-113862	Windows Network Address Translation (NAT)	Exécution de code à distance	Critique	8,1	n.d.
CVE-2026-119952	Windows Schannel	Exécution de code à distance	Critique	8,1	n.d.
CVE-2026-118148	Active Directory Domain Services	Élévation de privilèges	Critique	7,5	n.d.
CVE-2026-121663	Visual Studio Code	Contournement de sécurité	Importante	8,8	n.d.
CVE-2026-121662	Visual Studio Code	Exécution de code à distance	Importante	8,6	n.d.
CVE-2026-105501	Windows Installer	Élévation de privilèges	Importante	7,8	n.d.
CVE-2026-105524	Windows Management Instrumentation	Élévation de privilèges	Importante	7,8	n.d.

EPSS (FIRST) : aucun score publié au 10/11/2026 pour les failles de ce mois, d'où la mention « n.d. ». Les scores seront à consulter dans les prochains jours ; un score bas ne sera 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, exposition réseau sans authentification, score CVSS et appréciation de Microsoft (« exploitation plus probable »). Aucune probabilité mesurée (EPSS) n'était disponible ce mois-ci à la date de l'analyse.

01 **Outlook : usurpation, exploitée avant le correctif**

CVE-2026-124194 (modérée, CVSS 6,5)

Seule faille du mois exploitée, selon Microsoft et selon la CISA, qui l'a inscrite à son catalogue le 10/11. Classée seulement « modérée », elle est atteignable par le réseau sans compte, avec une action de l'utilisateur selon le vecteur publié. Concerne Microsoft 365 Apps et Office LTSC 2021 et 2024.

02 **Active Directory : LDAP, services de domaine et Kerberos**

CVE-2026-119958 (critique, CVSS 9,8) · CVE-2026-118146 (critique, CVSS 8,8) · CVE-2026-118148 (critique, CVSS 7,5) · CVE-2026-85844 (importante, CVSS 9,8)

LDAP : exécution de code critique notée 9,8, sans compte ni action de l'utilisateur, qui concerne aussi les postes Windows. Les deux failles des services de domaine, critiques, sont jugées « exploitation plus probable » par Microsoft. Kerberos : élévation de privilèges notée 9,8 sans compte, classée seulement « importante ». Compromettre un contrôleur de domaine, c'est compromettre tout le système d'information.

03 **DNS, DHCP, iSCSI et SQL Server : notées 9,8, mais seulement « importantes »**

CVE-2026-88218 (importante, CVSS 9,8) · CVE-2026-88243 (importante, CVSS 9,8) · CVE-2026-88234 (importante, CVSS 9,8) · CVE-2026-116945 (importante, CVSS 9,8)

Exécutions de code atteignables par le réseau sans compte ni action de l'utilisateur selon le vecteur publié. Microsoft les classe « importantes », mais leur score impose de les traiter comme des failles critiques, en commençant par les serveurs exposés.

04 **Exchange Server : exécution de code critique**

CVE-2026-118207 (critique, CVSS 8,8)

Jugée « exploitation plus probable » par Microsoft ; un compte de faible niveau suffit selon le vecteur publié. Concerne Exchange Server Subscription Edition. Un serveur Exchange est généralement exposé sur Internet, ce qui en fait une cible prioritaire.

05 **Windows Search et service réseau Xbox Live : exécutions de code critiques**

CVE-2026-116928 (critique, CVSS 9,8) · CVE-2026-112967 (critique, CVSS 9,8)

Notées 9,8, sans compte ni action de l'utilisateur selon le vecteur publié, sur des composants présents dans de nombreuses versions de Windows.

06 **Schannel et NAT Windows : exécutions de code critiques**

CVE-2026-119952 (critique, CVSS 8,1) · CVE-2026-113862 (critique, CVSS 8,1)

Atteignables sans compte et jugées « exploitation plus probable » par Microsoft. Schannel est le composant de Windows qui gère TLS : à traiter d'abord sur les serveurs exposés.

07 **Excel, Word, Outlook et PowerPoint : exécutions de code critiques**

CVE-2026-118292 (critique, CVSS 8,8) · CVE-2026-110047 (critique, CVSS 8,8) · CVE-2026-110043 (critique, CVSS 8,8) · CVE-2026-120005 (critique, CVSS 8,8)

Office concentre la plus grande part des failles critiques du mois (voir la lecture par environnement). Notées 8,8, elles demandent une action de l'utilisateur selon le vecteur publié. Avec la faille Outlook exploitée, la messagerie et les documents reçus sont le vecteur à surveiller ce mois-ci.

08 **Message Queuing : cinq exécutions de code critiques**

CVE-2026-116710 (critique, CVSS 8,1) · CVE-2026-119963 (critique, CVSS 8,1) · CVE-2026-119964 (critique, CVSS 8,1) · CVE-2026-109459 (critique, CVSS 8,1) · CVE-2026-119967 (critique, CVSS 8,1)

Sans compte ni action de l'utilisateur selon le vecteur publié, avec une complexité d'attaque élevée. Vérifier si le service MSMQ est activé : il peut l'être sans être utilisé.

09 **SharePoint Server Subscription Edition : trois failles notées 9 ou plus**

`CVE-2026-120002 (importante, CVSS 9,9) · CVE-2026-80095 (importante, CVSS 9,0) · CVE-2026-109454 (importante, CVSS 9,0)`

Élévations de privilèges et usurpation accessibles avec un simple compte, classées « importantes » malgré leur score. SharePoint peut héberger des documents sensibles.

10 **Hyper-V : élévations de privilèges critiques**

`CVE-2026-113753 (critique, CVSS 8,2) · CVE-2026-113856 (critique, CVSS 7,8) · CVE-2026-113865 (critique, CVSS 7,8)`

Microsoft classe plusieurs failles de l'hyperviseur « critiques » ce mois-ci. Une faille sur l'hyperviseur touche toutes les machines virtuelles qu'il héberge.

11 **Élévations de privilèges : Windows Installer, noyau, spouleur d'impression**

`CVE-2026-105501 (importante, CVSS 7,8) · CVE-2026-119892 (importante, CVSS 7,8) · CVE-2026-109473 (importante, CVSS 7,8) · CVE-2026-112811 (importante, CVSS 7,8)`

En l'absence de score EPSS, l'appréciation de Microsoft est le meilleur indicateur disponible : ces composants comptent plusieurs failles jugées « exploitation plus probable ». Une élévation de privilèges transforme un poste compromis en prise de contrôle complète.

12 **Visual Studio Code : exécutions de code sur les postes de développement**

`CVE-2026-120779 (importante, CVSS 9,6) · CVE-2026-121662 (importante, CVSS 8,6)`

Une faille notée 9,6 et une autre jugée « exploitation plus probable » par Microsoft. Les postes de développement détiennent souvent des accès sensibles (code source, secrets, déploiement).

Lecture par environnement

ENVIRONNEMENT	FAILLES	CRITIQUES	EXÉC. CODE	PLUS PROBABLES
Active Directory et identité Contrôleurs de domaine d'abord : LDAP et Kerberos sont atteignables sans compte, et une seule compromission suffit à prendre tout le domaine.	24	3	3	2
Exchange Server Une faille critique jugée « exploitation plus probable » : serveurs à mettre à jour dans les 72 heures.	9	1	2	1
SharePoint Aucune faille critique, mais trois scores de 9 ou plus ; priorité aux fermes publiées sur Internet.	27	0	6	0
Office et Outlook La faille exploitée et le plus grand nombre de failles critiques : déployer sur tous les postes par l'outil de gestion habituel.	174	22	148	0
Services réseau (DNS, DHCP, IIS, SMB, TLS, MSMQ…) Le plus grand nombre de failles atteignables sans compte ni action de l'utilisateur : commencer par les serveurs exposés.	122	13	40	7
SQL Server Aucune faille classée critique, mais une exécution de code notée 9,8 sans compte : à ne pas laisser au cycle normal.	54	0	20	0
.NET, Visual Studio et VS Code Penser aux serveurs d'applications et aux postes de développement ; .NET 8 arrive en fin de support ce mois-ci.	48	0	12	2

Hyper-V et virtualisation Plusieurs élévations de privilèges critiques : une faille sur l'hyperviseur touche toutes les machines virtuelles qu'il héberge.	16	8	0	0
Noyau, pilotes et Windows Installer Surtout des élévations de privilèges, souvent jugées « plus probables » : elles servent à la seconde étape d'une attaque.	204	3	12	13

Fins de support à ne pas manquer

- .NET 8 (LTS) : fin du support le 10/11/2026.
- .NET 9 : fin du support le 10/11/2026 selon la politique de support .NET de Microsoft ; la page Microsoft des fins de support 2026 indique encore le 12/05/2026.
- PowerShell 7.4 (LTS) : fin du support le 10/11/2026.
- Windows 11 Entreprise et Éducation et Windows 11 IoT Entreprise, version 23H2 : fin du support le 10/11/2026.
- Azure IoT Edge 1.5 (LTS) et modèle « in-process » d'Azure Functions : fin du support le 10/11/2026.
- Rappel : Office LTSC 2021, Office 2021 et Windows 11 Famille et Professionnel, version 24H2, sont déjà hors support depuis le 13/10/2026. Microsoft liste encore Office LTSC 2021 parmi les produits concernés par CVE-2026-124194 : appliquer le correctif disponible et planifier la migration.

Plan de déploiement recommandé

Sous 72 h	**Faille exploitée, identité et serveurs exposés** CVE-2026-124194 sur tous les postes Outlook ; contrôleurs de domaine (LDAP, Kerberos, services de domaine) ; Exchange ; DNS, DHCP, Windows Search, service réseau Xbox Live et serveurs publiés sur Internet.
Sous 7 jours	**Postes et cœur de l'infrastructure** Office sur tous les postes ; Windows (Message Queuing, Schannel, NAT) ; SQL Server, SharePoint, Hyper-V, iSCSI.
Sous 30 jours	**Le reste du parc** Serveurs internes, Visual Studio Code et postes de développement ; migration des versions arrivées en fin de support ; 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 10/11/2026, soit 1 093, lues dans les données officielles de Microsoft (CVRF) mises à jour au 10/11/2026 ; les publications anticipées du début du mois

en sont exclues. Gravité : la plus élevée attribuée par Microsoft parmi les produits concernés. Exploitation : catalogue CISA KEV (version 10/11/2026) et indicateurs de Microsoft. Probabilité : aucun score EPSS n'était publié au 10/11/2026, d'où la mention « n.d. » ; les priorités ne s'appuient donc pas sur l'EPSS ce mois-ci. Les fins de support sont vérifiées sur les sites officiels de Microsoft (cycle de vie et politique de support .NET). La situation évolue : ce rapport décrit l'état au 10/11/2026.

Sources

- Microsoft MSRC · notes de version de novembre 2026 / November 2026 release notes
  https://msrc.microsoft.com/update-guide/releaseNote/2026-Nov
- Microsoft MSRC · données CVRF / CVRF data
  https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Nov
- 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
- Microsoft · politique de support .NET / .NET support policy
  https://dotnet.microsoft.com/en-us/platform/support/policy/dotnet-core