



> Consultez le paysage passé, présent et à venir des vulnérabilités Microsoft

Microsoft Vulnerabilities Report 2023

Une décennie de renseignements sur les vulnérabilités pour aider les organisations à améliorer leur cyberdéfense où qu'elles se trouvent

ÉDITION
ANNIVERSAIRE





TABLE DES MATIÈRES

Résumé analytique	3
Données marquantes et principales conclusions	4
Microsoft au cours de la décennie	5
Comprendre les vulnérabilités critiques	8
Données rétrospectives du rapport	11
Analyse détaillée des données sur les vulnérabilités	14
L'effet boule de neige des vulnérabilités	26
Qu'en dit ChatGPT ?	28
Qu'en disent les experts ?	31
Atténuer les risques de vulnérabilité liés à Microsoft	39
Conclusion	41
Méthodologie	42
Ressources supplémentaires	43



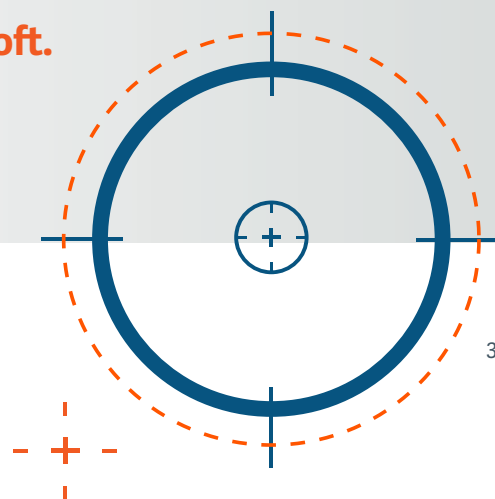
Le Microsoft Vulnerabilities Report célèbre fièrement son dixième anniversaire.

Le rapport, depuis sa première publication en 2013, a été téléchargé plus de 15 000 fois et a profité à des milliers d'utilisateurs grâce à ses analyses de données détaillées et à ses conclusions d'experts.

L'édition pour le dixième anniversaire du rapport analyse les données de 2022 sur les vulnérabilités Microsoft et met en évidence certaines évolutions clés depuis la création du rapport. Ce rapport mettra en lumière certaines des CVE (Common Vulnerabilities and Exposures) les plus importantes de 2022 (niveaux de gravité selon le Common Vulnerability Scoring System ou CVSS de 9 ou plus), détaillera la façon dont elles sont exploitées par les attaquants et expliquera comment elles peuvent être évitées ou atténuées.

Un panel composé des plus grands experts mondiaux en cybersécurité se prononcera sur les conclusions du rapport. Il y aura aussi un invité spécial, expert de l'IA, qui interviendra dans le cadre de notre réflexion sur les menaces, les vulnérabilités et les cyberdéfenses de la prochaine décennie.

Poursuivez votre lecture pour mieux comprendre, identifier et traiter les risques au sein de l'écosystème Microsoft.





Données marquantes et principales conclusions

En 2022, le nombre total de **vulnérabilités Microsoft a atteint 1 292, établissant un record** depuis la première publication du rapport il y a 10 ans.

Cependant, ce n'est pas seulement le nombre de vulnérabilités qui doit nous préoccuper, **mais aussi la menace unique et l'impact** que représentent les vulnérabilités individuelles.

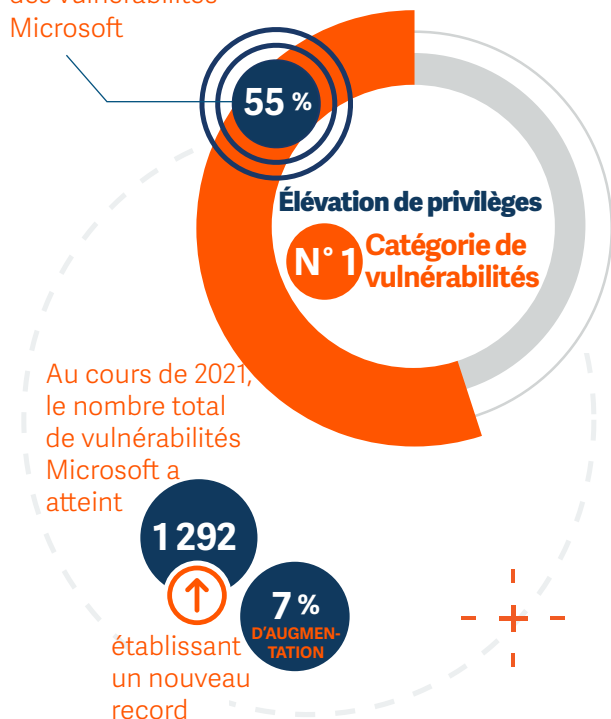
1

La **catégorie de l'élévation des privilèges domine** le paysage des vulnérabilités de Microsoft pour la troisième année consécutive et continue de progresser.

2

Microsoft Azure et Dynamics 365 sont les environnements **générant le plus de profit pour Microsoft**, mais ils **génèrent aussi le plus de vulnérabilités**.

L'élévation des privilèges représente **55 % du total** des vulnérabilités Microsoft



Les vulnérabilités critiques ont baissé pour la deuxième année consécutive, **atteignant 89 en 2022, le niveau le plus bas sur cinq ans**.

En 2022, 6,9 % des vulnérabilités Microsoft étaient classées comme « critiques », tandis qu'en 2013, 44 % de toutes les vulnérabilités Microsoft étaient classées comme « critiques ».

Les vulnérabilités Azure et Dynamics 365 ont explosé en augmentant de 159 %, passant de 44 en 2021 à 114 en 2022.

Microsoft Edge a connu 311 vulnérabilités l'année dernière, mais **aucune n'était critique**.

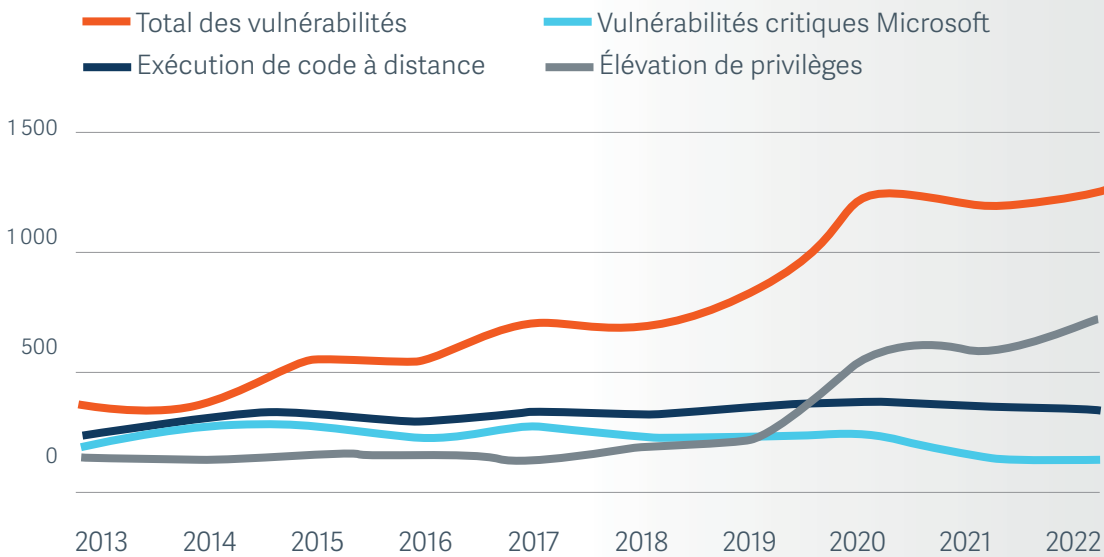
Il y a eu **513 vulnérabilités Windows en 2022**, dont 49 étaient critiques.

Microsoft Office a atteint **son plus bas sur cinq ans avec seulement 36** vulnérabilités en 2022.

Les vulnérabilités Windows Server ont légèrement augmenté pour atteindre 552 en 2022.



Un aperçu de Microsoft sur la décennie (2013 – 2022)





Microsoft : D'hier à aujourd'hui

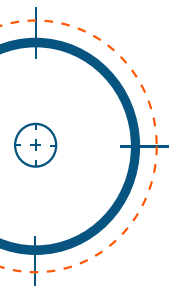
	2013	2022
Capitalisation boursière (en USD, au 31 décembre)	314 milliards USD	1,79 billion USD
Nombre de clients Microsoft au niveau mondial (Données 2013 pour l'exercice 2013 ; Données 2022 exactes au 24 octobre 2022)	1,5 milliard d'utilisateurs Windows dans le monde Plus d'un million d'abonnés à Office 365 Famille Premium	1,4 milliard d'appareils actifs mensuels fonctionnant sous Windows 10/11 60 millions d'abonnements grand public à Microsoft 365 ; 25 millions d'utilisateurs actifs mensuels sur Power Platform ; 270 millions d'utilisateurs actifs mensuels sur Teams
PDG de Microsoft	Steve Ballmer	Satya Nadella
Top des produits phares (basé sur le % d'augmentation du CA au cours de l'exercice)	Office 2013 Windows 8.1	Windows 11 Datacenter Windows Server 2022 : Azure Edition SQL Server 2022
Top des acquisitions	Nokia (7,2 milliards USD)	Activision (l'acquisition de 70 milliards USD fut la plus importante jamais réalisée dans l'industrie du jeu et la plus importante jamais réalisée par Microsoft)
Produits représentant la plus grande part des revenus de Microsoft	Produits Office (23 milliards USD en 2013)	Produits pour serveur et services dans le cloud (67,3 milliards USD lors de l'exercice 2022)
Revenus tirés du cloud intelligent	15,4 milliards USD (classés comme revenus des produits pour serveur et services dans le cloud)	65,29 milliards USD
Mantra	2013 a vu l'ajout de la « création d'une famille d'appareils » dans son objectif commercial et a déclenché la vision « One Microsoft »	« Intelligent Cloud » annoncé en mai 2017 et remplaçant « Mobile First, Cloud First », annoncé en mai 2014
Comment la sécurité et la confidentialité sont structurées chez Microsoft	La Trustworthy Computing Unit (TwC) a centralisé les pratiques en matière de confidentialité et de sécurité chez Microsoft	Les responsabilités en matière de sécurité et de confidentialité sont intégrées à l'ensemble de l'entreprise (la TwC a été démantelée en 2014)
Méthodologie de signalement des vulnérabilités Microsoft	Partage des détails sur les CVE (Common Vulnerabilities and Exposures) via le guide de mise à jour sur la sécurité de Microsoft	Système standardisé CVSS (Common Vulnerability Scoring System) (adopté en novembre 2020). Le passage au système CVSS a permis de simplifier les références croisées avec des bugs tiers, mais la modification du format de rapport a également indiqué que l'impact des droits d'admins sur les vulnérabilités critiques ne pouvait pas être clairement déterminé.
Nombre total de vulnérabilités Microsoft	333	1 292



	2013	2022
Nombre total de vulnérabilités critiques Microsoft	147	89
Catégorie de vulnérabilités Microsoft n° 1	Exécution de code à distance	Élévation de privilèges
Gammes de produits avec le plus de vulnérabilités	Microsoft Windows Server (252) Systèmes d'exploitation Windows XP, Vista, Windows 7 et Windows 8 (252)	Microsoft Windows Server (552), Microsoft Windows (513), Microsoft Edge (311), Azure et Dynamics 365 (114)
Vulnérabilités récurrentes (Vulnérabilités qui se reproduisent ou mettent des années à être complètement résolues, dans ce cas les 10 années couvertes par ce rapport)	CVE-2013-3900 (Une vulnérabilité liée à l'exécution de code à distance causée lorsque la fonction WinVerifyTrust valide de manière incorrecte le fichier condensé d'un fichier PE spécialement conçu lors de la vérification d'une signature Windows Authenticode)	La vulnérabilité de 2013 a été republiée par Microsoft en 2022 pour informer les clients qu'une mise à jour de Windows 10/11 la corrigeait.

Alors, qu'est-ce qui a changé ?

- Le besoin d'un programme efficace de gestion des vulnérabilités (recherche, hiérarchisation et correction des vulnérabilités)
- La nécessité de supprimer les droits admins et d'appliquer le principe du moindre privilège pour atténuer proactivement les vulnérabilités





Comprendre les vulnérabilités critiques de Microsoft

Bien que le nombre total de vulnérabilités soit une mesure importante pour évaluer la santé d'un environnement, comme nous l'aborderons dans ce rapport, les vulnérabilités ne sont pas toutes égales entre elles.

Certaines vulnérabilités peuvent représenter principalement un risque théorique (faible probabilité) et un faible impact si elles sont exploitées, tandis qu'à l'opposé du spectre, d'autres vulnérabilités ont une forte probabilité d'être exploitées, auquel cas un impact très négatif sur les organisations affectées peut se produire.

La mesure de l'impact d'une vulnérabilité sera liée à ses conséquences sur la confidentialité, l'intégrité et la disponibilité des données au sein d'un système ou d'une organisation. Les vulnérabilités les plus graves auront un impact sur ces trois aspects fondamentaux de la sécurité des informations.

Les vulnérabilités classées comme « critiques » produisent un événement de sécurité à fort impact potentiel lorsqu'elles sont exploitées.

La façon dont Microsoft détermine le niveau de gravité d'une vulnérabilité est distincte de la probabilité qu'elle soit exploitée. Cependant, la probabilité d'exploitation est bien plus dynamique car, généralement, les attaquants sont beaucoup plus susceptibles d'exploiter une vulnérabilité connue.

L'exploitation de vulnérabilités « critiques » :

Compromettra probablement tout un appareil ou toute une infrastructure.

Aura moins de prérequis.
Habituellement, l'attaque ne nécessite aucun accès spécial, aucun privilège ni aucune connaissance avancée.

Permet des exécutions de code sans interaction de l'utilisateur. Celles-ci ne reposent généralement pas sur une méthode d'ingénierie sociale ciblant un utilisateur.

→ **Ce sont les types de vulnérabilités qui donnent des cauchemars aux administrateurs informatiques et présentent le plus de risques et de défis pour les entreprises.**



Quelle est la méthode de classement des vulnérabilités critiques employée par Microsoft ?

La Base de données nationale des vulnérabilités (NVD) considère des vulnérabilités comme critiques lorsqu'elles obtiennent un score de 9 à 10 en vertu du [CVSS \(Common Vulnerability Scoring System\)](#). Les lecteurs les plus assidus des annonces de Microsoft concernant les vulnérabilités ont peut-être remarqué que, bien que Microsoft utilise désormais le système CVSS 3.1 pour noter celles-ci, les gravités sont déterminées en fonction du propre Security Update Severity Rating System de Microsoft. Ce système classe chaque vulnérabilité selon le pire résultat théorique, en cas d'exploitation.

→ **Cela signifie que, alors que seules 22 vulnérabilités Microsoft ont obtenu un score de neuf ou plus (ce qui les rend « critiques » selon le système de notation de la base de données nationale sur les vulnérabilités) à partir de 2022, Microsoft a classé 89 de ses vulnérabilités comme étant critiques.**

Notations CVSS 3.1

Gravité	Plage de scores de base
Inexistante	0
Faible	0,1 - 3,9
Moyenne	4 - 6,9
Élevée	7 - 8,9
Critique	9 - 10

Notation Description

Critique	Une vulnérabilité dont l'exploitation pourrait permettre des exécutions de code sans interaction de l'utilisateur. Ces scénarios incluent du malware se propageant automatiquement (par exemple, des vers de réseau) ou des scénarios d'utilisation courante inévitables dans lesquels une exécution de code se produit sans avertissement. Cela peut concerner la navigation sur une page Web ou l'ouverture d'un e-mail. Microsoft recommande à ses clients d'appliquer immédiatement les mises à jour critiques.
Importante	Une vulnérabilité dont l'exploitation pourrait compromettre la confidentialité, l'intégrité ou la disponibilité des données utilisateur, ou l'intégrité ou la disponibilité des ressources de traitement. Ces scénarios incluent ceux d'utilisation courante où le client est compromis avec des avertissements et des notifications, indépendamment de la provenance, de la qualité ou de la facilité d'utilisation de ces derniers. Les séquences d'actions de l'utilisateur qui ne génèrent pas d'invites ou d'avertissements sont également concernées. Microsoft recommande à ses clients d'appliquer dès que possible les mises à jour importantes.
Modérée	L'impact de la vulnérabilité est atténué de façon significative au moyen de facteurs tels que les exigences d'authentification ou l'applicabilité uniquement à des configurations autres que par défaut. Microsoft recommande à ses clients d'appliquer la mise à jour de sécurité.
Faible	L'impact de la vulnérabilité est atténué de manière exhaustive par les caractéristiques du composant affecté. Microsoft recommande à ses clients d'évaluer le fait d'appliquer ou non la mise à jour de sécurité sur les systèmes affectés.

Le système de classement de la gravité de Microsoft est susceptible d'offrir de meilleures perspectives pour la priorisation de la réduction des risques.



La différence entre les scores CVSS et le système de classement de la gravité de Microsoft est intéressante à noter, non seulement en considérant les données dans ce rapport, mais aussi en appréhendant le risque dans votre organisation.

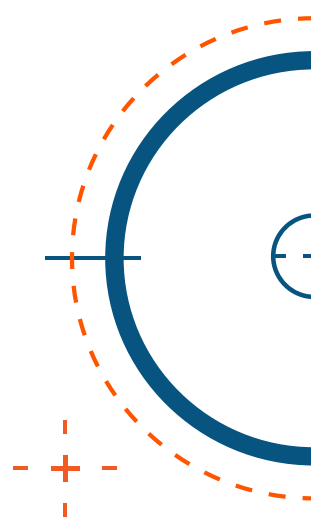
Le score CVSS mesure la gravité technique d'une vulnérabilité.

Par exemple, le fait de savoir si une vulnérabilité entraîne une perte de confidentialité des données partielle ou totale. Le score CVSS ne mesure pas le risque de cette vulnérabilité. Cela signifie que les scores CVSS ne permettent pas à eux seuls de savoir si une vulnérabilité aura un impact critique sur un système, ou si la perte limitée de certaines données très sensibles aura un impact plus important que la perte totale de données non sensibles.

Le système de classement de la gravité de Microsoft est potentiellement bien plus utile qu'un score CVSS de base ou temporel pour les spécialistes de la sécurité qui tentent d'établir des priorités en matière de réduction des risques. Toutefois, il est important de connaître votre propre environnement et vos propres risques afin de comprendre comment prioriser au mieux les correctifs et/ou utiliser d'autres mesures d'atténuation et de contrôle pour renforcer la sécurité.

Toutes les données fournies par le système de classement de la gravité de Microsoft sont basées sur les informations qui étaient alors disponibles et ne prennent pas en compte le contexte des modèles de menaces de votre propre organisation. Ce qui est considéré comme un correctif critique pour une organisation peut ne pas l'être pour une autre : tout dépend du contexte de l'entreprise.

Outre son [Security Update Severity Rating System](#), Microsoft a également publié un [Exploitability Index](#) pour aider ses clients à déterminer la probabilité d'une exploitation. Cela peut être une information utile pour ceux qui ont besoin d'aide afin de prioriser les mises à jour de sécurité. À titre d'avertissement, ces informations reflètent la probabilité d'exploitation au moment de la publication de la mise à jour de sécurité. Elles peuvent ne pas refléter l'exploitabilité réelle qui se développe au cours des semaines ou des mois suivants, à mesure que les acteurs malveillants exploitent la vulnérabilité. L'index est plus utile pour la priorisation à très court terme des mises à jour plutôt que comme justification pour retarder significativement l'application de correctifs.



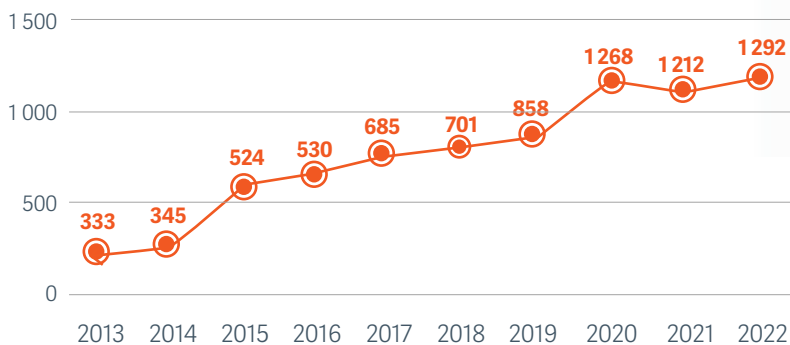


Données rétrospectives du rapport

Un résumé sur dix ans

Voici la façon dont les conclusions de cette année en matière de vulnérabilités Microsoft s'alignent sur les tendances des dix dernières années.

Nombre total de vulnérabilités Microsoft (2013 - 2022)



Le nombre total de vulnérabilités Microsoft a atteint un niveau record, mais se stabilise-t-il sur le long terme ?

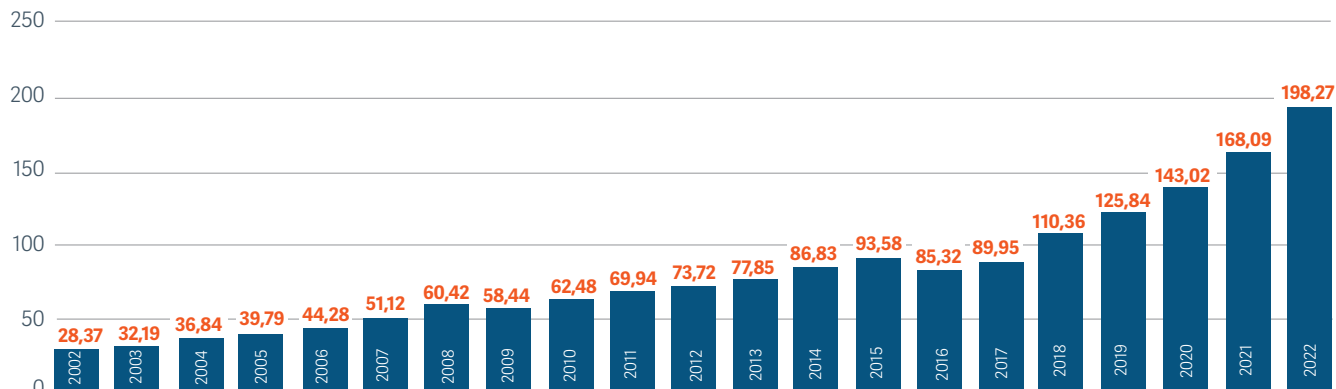
Un nouveau record pour le nombre de vulnérabilités Microsoft a été enregistré en 2022, dépassant de 2 % le précédent record établi en 2020. Cependant, si nous regardons la tendance sur le plus long terme, nous pouvons voir que le nombre de vulnérabilités semble plafonner quelque peu après des années de croissance significative.

Pourquoi constatons-nous cette tendance ? Pour paraphraser le rappeur The Notorious B.I.G., « Plus d'argent, c'est plus de problèmes », ce qui semble bien être le cas de Microsoft. Pour augmenter son chiffre d'affaires, Microsoft a créé de nouveaux produits et amélioré ceux qui existent déjà. Ce faisant, ces nouvelles offres augmentent potentiellement la surface d'attaque en fournissant un nouveau code.

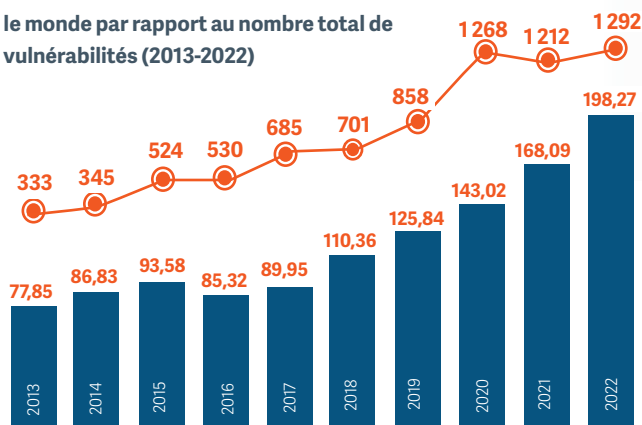
En outre, plus vous avez de clients, plus il y a de personnes qui examinent votre logiciel, des équipes de recherche internes aux testeurs externes, en passant par les pays mal intentionnés et les cybercriminels.



Chiffre d'affaires annuel de Microsoft dans le monde de 2002 à 2022 (en milliards USD)



Chiffre d'affaires annuel de Microsoft dans le monde par rapport au nombre total de vulnérabilités (2013-2022)



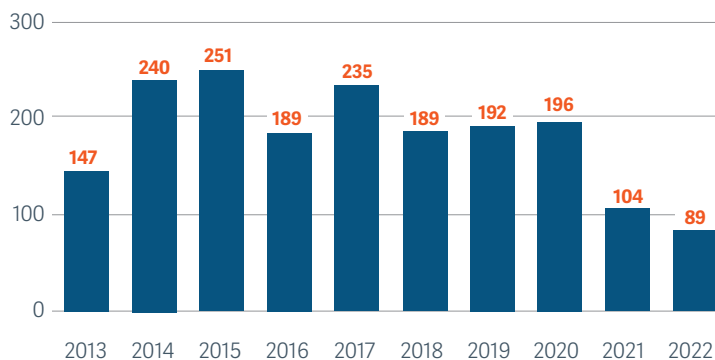
Le chiffre d'affaires total et l'ensemble des vulnérabilités Microsoft ont doublé entre 2017 et 2020.

Alors, « plus d'argent », est-ce vraiment « plus de problèmes » ? Bien que ce ne soit pas une mesure exacte, si nous examinons le chiffre d'affaires global de Microsoft de 2013 à 2022 et que nous le comparons au nombre total de vulnérabilités Microsoft, nous pouvons observer une tendance similaire, le chiffre d'affaires et les vulnérabilités doublant presque entre 2017 et 2020.

De plus, si nous nous intéressons aux gammes de produits avec la plus forte croissance, nous voyons que Microsoft Azure et Dynamics 365 procurent non seulement les gains financiers les plus importants pour l'entreprise (les revenus du cloud représentaient 51,4 % du chiffre d'affaires total de Microsoft en 2022), mais représentent également la plus forte croissance de vulnérabilités, à la fois en raison de l'accroissement de leur nombre (70) et du pourcentage d'augmentation (159 %) en 2022.



Vulnérabilités critiques Microsoft (2013-2022)



Le nombre de vulnérabilités critiques de Microsoft a atteint son point le plus bas au cours des 10 années couvertes par ce rapport.

Les vulnérabilités critiques de Microsoft ont baissé de 55 % depuis 2020, ce qui indique une réduction du niveau global de risque associé aux vulnérabilités individuelles.

Deux records ont été atteints en ce qui concerne les vulnérabilités dans la dixième édition du rapport, ce qui semble souligner des tendances contraires. Alors que le nombre total de vulnérabilités Microsoft a atteint son plus haut niveau enregistré en 2022, le nombre de vulnérabilités critiques a atteint son niveau le plus faible, avec moins de la moitié d'entre elles en 2022 par rapport à 2020. En 2022, 6,9 % des vulnérabilités Microsoft seulement étaient classées comme « critiques », tandis qu'en 2013, 44 % de toutes les vulnérabilités Microsoft étaient classées comme « critiques ».

Cette tendance indique que, si les vulnérabilités globales ont augmenté en nombre, les risques et les pires scénarios associés à ces vulnérabilités individuelles ont baissé par rapport aux années précédentes. Cela indique également que, si la surface d'attaque globale de Microsoft s'étend de concert avec l'expansion de ses activités, l'entreprise parvient mieux à minimiser les types d'erreurs de développement les plus dangereux.

Microsoft a réalisé des investissements significatifs pour améliorer la sécurité au fil des années. Nous pensons que cela se reflète dans la tendance à la baisse du nombre de vulnérabilités critiques de Microsoft.

De nombreux produits Microsoft ont bénéficié d'un support sur une très longue durée, ce qui signifie que ces améliorations de la sécurité se produisent à mesure que les organisations passent à des produits plus récents et plus sûrs, ainsi qu'à davantage d'instances SaaS, où la dernière version est mise à la disposition de chacun.



À mesure que le nombre de vulnérabilités critiques baisse, les attaquants peuvent avoir besoin d'enchaîner plusieurs failles d'une gravité moindre pour déclencher l'exécution d'un code, élever les privilèges et se déplacer sur le réseau.

Du point de vue du défenseur, c'est une bonne chose, car cela requiert un meilleur niveau de compétences de la part de l'attaquant et réduit le nombre d'adversaires potentiels. Cela fournit également plus d'opportunités pour détecter, intercepter et atténuer une menace.

Si un attaquant doit exploiter simultanément trois vulnérabilités ou plus pour atteindre son objectif, il vous suffit de remédier à l'une d'elles ou de la corriger pour briser la chaîne.



Analyse détaillée des données sur les vulnérabilités

L'exécution de code à distance et l'élévation de privilèges continuent d'être les principales catégories de vulnérabilités.



Vulnérabilités par catégorie

Chaque bulletin de sécurité de Microsoft porte sur une ou plusieurs vulnérabilités affectant un ou plusieurs produits Microsoft. Microsoft répartit généralement les vulnérabilités dans ces catégories principales : **exécution de code à distance (RCE), élévation de privilèges (EoP), divulgation d'informations, déni de service (DoS), usurpation, falsification et contournement des fonctions de sécurité.**

En 2022, l'élévation de privilèges et l'exécution de code à distance ont continué de dominer les autres catégories de vulnérabilités.

Cela mis à part, les vulnérabilités liées aux élévations de privilèges continuent de croître à un rythme soutenu, tandis que les vulnérabilités concernant l'exécution de code à distance ont légèrement diminué au cours des trois dernières années.

Les vulnérabilités associées aux élévations des privilèges ont grimpé en flèche en 2022 pour atteindre un total de 715, soit une augmentation de 22 % par rapport à 2021 et une progression gigantesque de 689 % depuis 2017.

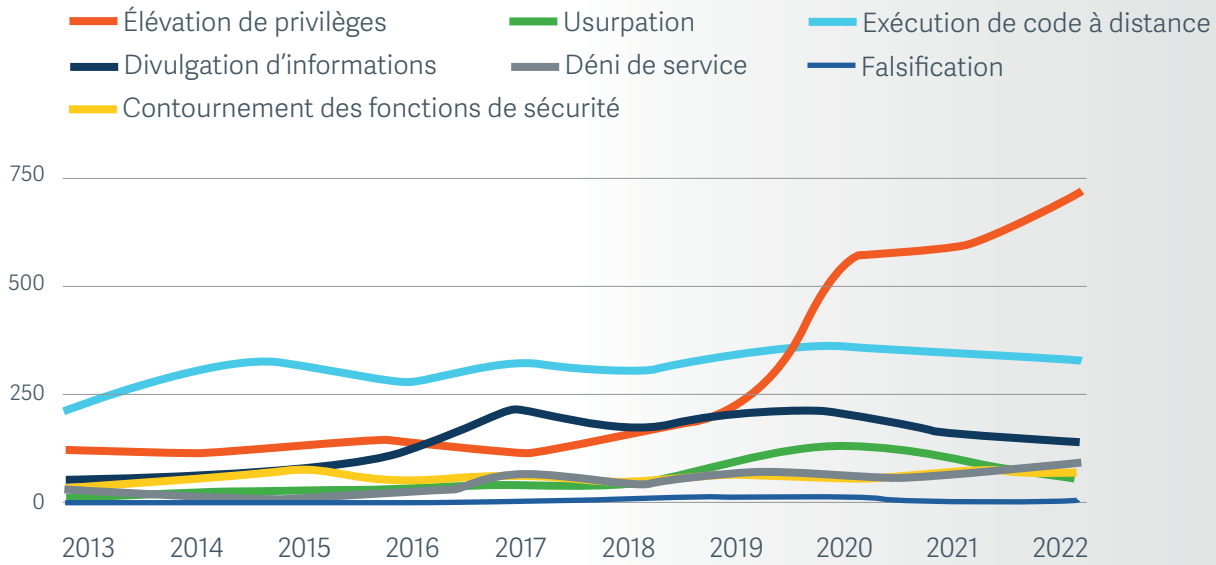
L'exécution de code à distance a poursuivi sa légère tendance à la baisse depuis le pic observé en 2020, diminuant de 4 % en 2022 avec une chute de 5,5 % en 2021.

Catégories de vulnérabilités Microsoft (2013-2022)

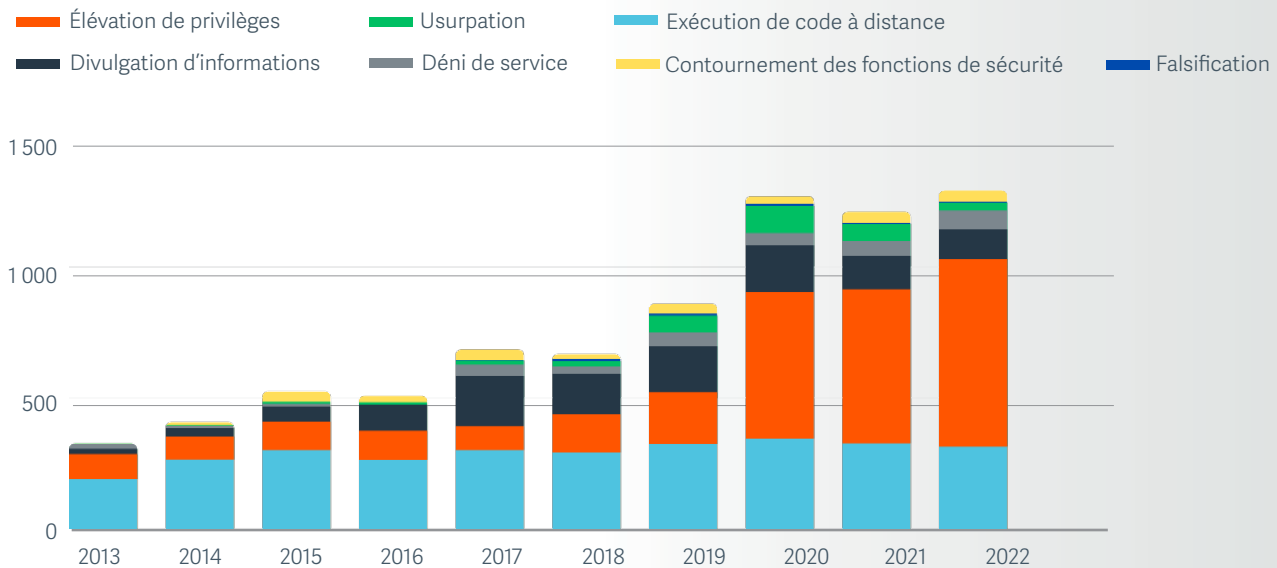
	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Exécution de code à distance	190	264	301	262	301	292	323	345	326	314
Élévation de privilèges	95	87	107	112	90	145	198	559	588	715
Divulgation d'informations	20	34	59	99	193	153	177	179	129	114
Déni de service	18	7	9	0	43	29	52	46	55	72
Usurpation	2	3	8	10	16	20	63	104	66	31
Falsification	0	0	0	0	1	8	8	7	3	4
Contournement des fonctions de sécurité	0	12	40	25	41	20	38	30	44	42



Catégories de vulnérabilités Microsoft (2013-2022)

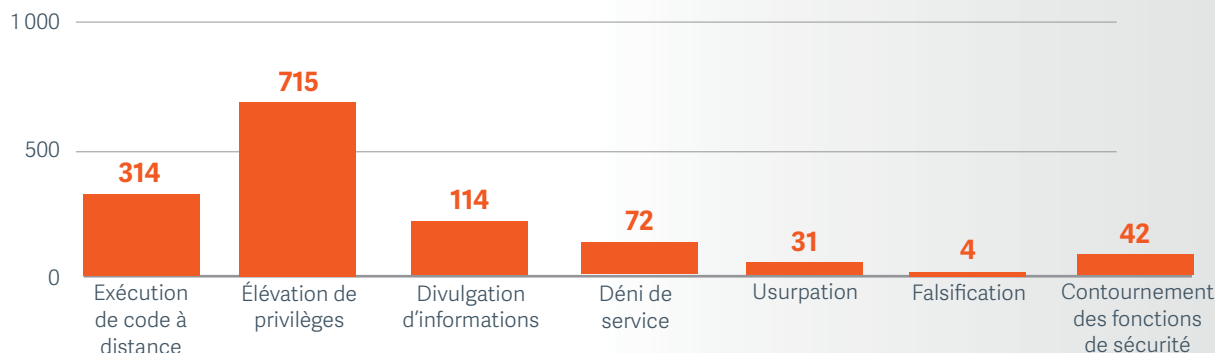


Catégories de vulnérabilités Microsoft (2013-2022)





Répartition des catégories de vulnérabilités Microsoft (2022)



Que nous indiquent les catégories de vulnérabilités ?

Bien que les niveaux de vulnérabilités changent, les objectifs des acteurs malveillants restent les mêmes, en privilégiant l'exécution de code à distance et l'élévation de privilèges.

Comme nous l'avons mentionné plus haut dans ce rapport, la réduction des vulnérabilités critiques signifie que les attaquants peuvent moins facilement compromettre totalement un système en une seule fois. C'est une bonne nouvelle pour les organisations mais l'objectif d'un attaquant demeure inchangé : provoquer l'exécution de son code et s'assurer qu'il s'exécute avec suffisamment de privilèges pour parvenir à ses fins.

Pour atteindre cet objectif, les attaquants doivent pouvoir exécuter un code à distance, le lancer sur un système cible et élever les privilèges pour s'assurer que ce code s'exécute avec un nombre suffisant d'entre eux. Cela se reflète dans la conclusion que l'exécution de code à distance et l'élévation de privilèges restent les catégories de vulnérabilités Microsoft les plus importantes, comme le souligne ce rapport. Le nombre de vulnérabilités liées aux élévations de privilèges dans l'environnement Microsoft a notamment connu une forte croissance au cours des trois dernières années.

Les données de ce rapport indiquent qu'en 2022, Microsoft continue de réduire le nombre de vulnérabilités critiques et de supprimer des privilèges excessifs, en particulier sur les endpoints. Les attaquants ont de ce fait besoin d'exploiter les vulnérabilités associées aux élévations de privilèges pour réussir.

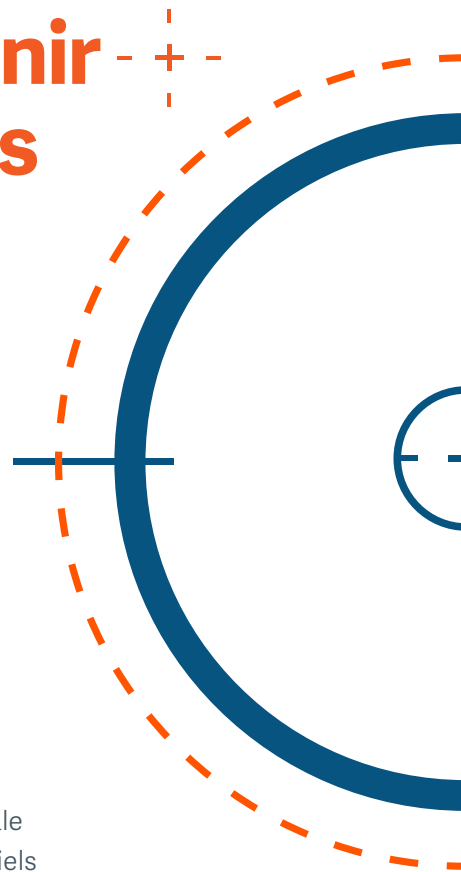


Deux principaux enseignements en matière de sécurité à retenir au regard des données sur les catégories de vulnérabilités

- 1** Vérifiez toujours que votre système d'exploitation et vos logiciels tiers sont à jour et que vous n'utilisez pas de logiciels en fin de vie dans votre environnement.
- 2** Assurez-vous de constamment supprimer les privilèges excessifs, en particulier sur les endpoints.

Sans surprise, les [CIS Controls du SANS Institute](#), les [Essential 8 Cyber Risk Controls](#) de l'Australian Cyber Security Centre (ACSC) et l'[architecture Zero Trust](#) (publication spéciale 800-207) du NIST soulignent aussi que ces contrôles en matière de sécurité sont essentiels pour la prévention et l'atténuation des menaces.

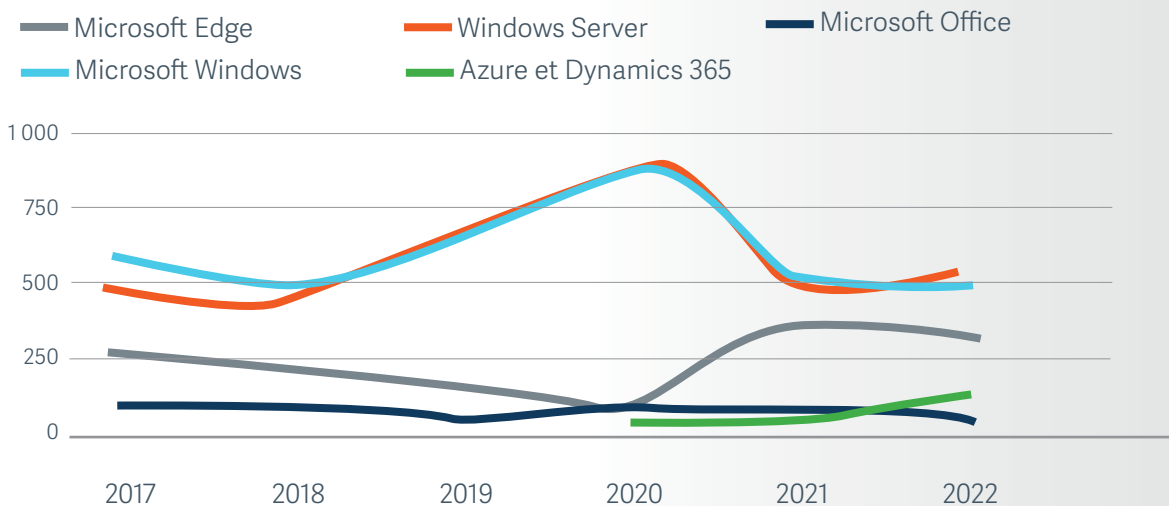
Consultez la section « Atténuation des risques posés par les vulnérabilités associées à Microsoft » en fin de rapport pour obtenir de plus amples renseignements.



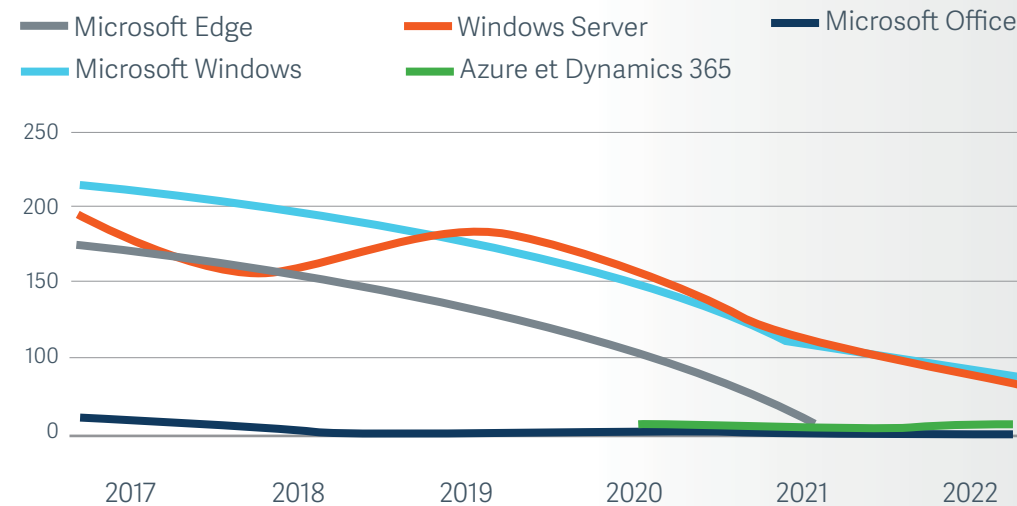


Vulnérabilités par produit

Vulnérabilités par produit (2017-2022)

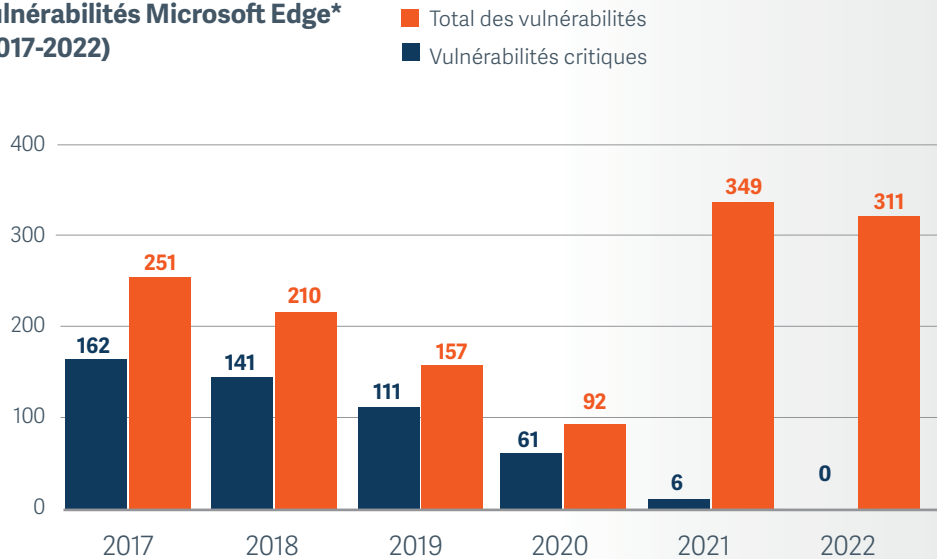


Vulnérabilités critiques par produit (2017-2022)





Vulnérabilités Microsoft Edge* (2017-2022)



La période 2017-2021 inclut Internet Explorer qui n'est plus pris en charge depuis l'an dernier. Les chiffres de 2022 concernent uniquement Edge.

Après avoir presque quadruplé en 2021, le nombre total de vulnérabilités Microsoft Edge a diminué de 11 % pour atteindre un chiffre de 311 en 2022 tandis que les vulnérabilités critiques ont continué de chuter

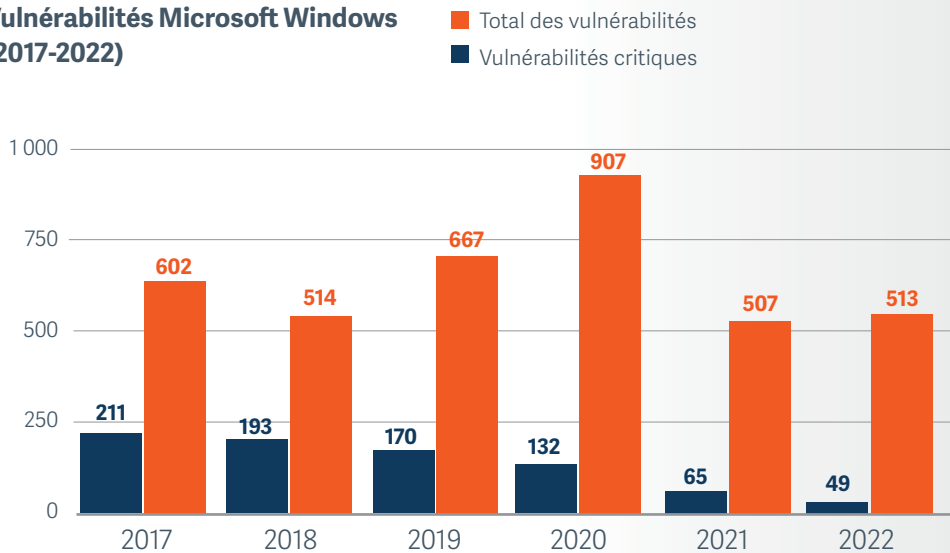
Ceux qui ne sont pas familiers avec ce qui s'est passé dans les entrailles d'Edge au cours des dernières années peuvent s'interroger sur les motifs de la baisse soudaine des vulnérabilités critiques et de la hausse du nombre total de vulnérabilités en 2020. Ces motifs se rapportent au fait que Microsoft a abandonné son propre moteur de navigation et a repensé Edge autour de Chromium. Les avantages de cette décision étaient que Microsoft peut désormais s'appuyer sur le moteur Chromium, plus mature et open source, pour résoudre ses problèmes de vulnérabilités critiques, ainsi que toute une série de problèmes de compatibilité qui poussaient souvent les clients à n'utiliser Edge qu'une seule fois, en téléchargeant le programme d'installation de Chrome.

Le projet Chromium a l'avantage d'être en open source et suffisamment omniprésent pour attirer l'attention de la communauté des chercheurs en sécurité. Cette situation lui a permis de mûrir rapidement. Les autres navigateurs ne sont pas nécessairement plus sûrs, bien qu'ils puissent avoir un nombre global de vulnérabilités inférieur à Edge (ou Chrome).

Les tendances en matière de vulnérabilités du navigateur Edge illustrent parfaitement ce qui arrive lorsque les choses se compliquent pour un attaquant. Une vulnérabilité critique dans un navigateur peut permettre à un attaquant de provoquer une exécution privilégiée sur un système simplement en incitant la victime à cliquer sur un lien malveillant. Cependant, les attaquants, n'ayant pas de solution facile, doivent exploiter simultanément plusieurs vulnérabilités moins graves pour aller d'un point A à un point B.



Vulnérabilités Microsoft Windows (2017-2022)



Les vulnérabilités critiques Windows continuent de chuter, suite à la fin de vie de Windows 7 et au passage à la sécurité basée sur la virtualisation (VBS).

En 2020, la fin de la prise en charge de Windows 7 a obligé les utilisateurs à passer au système d'exploitation Windows 10 qui a supprimé de nombreuses vulnérabilités connues. Cela explique la baisse nette de 44 % du nombre de vulnérabilités de Microsoft Windows entre 2020 et 2021.

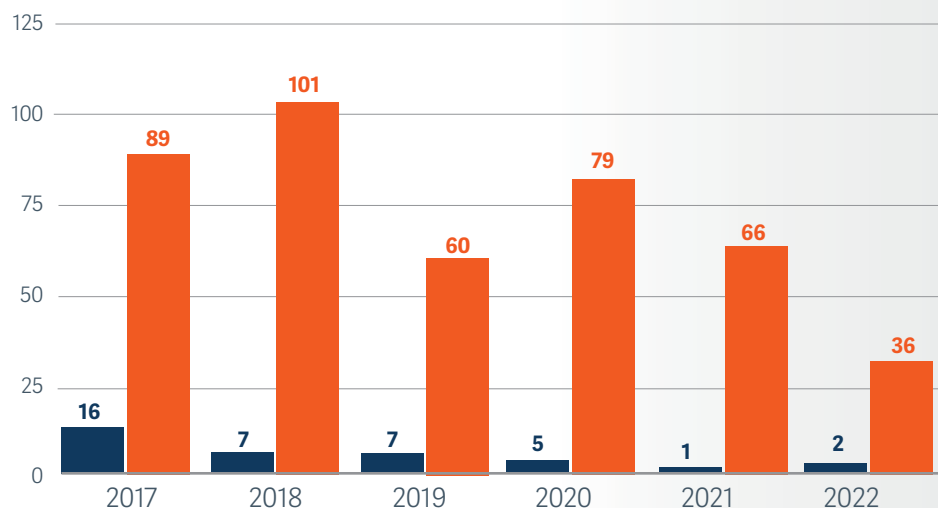
Windows 10 existe depuis environ 2015 et Windows 11, bien que lancé seulement en 2021, partage la même ossature que son prédécesseur. Cela signifie que ce système d'exploitation est moins susceptible de présenter de nouvelles vulnérabilités importantes. En outre, certains problèmes de sécurité ont été corrigés en utilisant la sécurité basée sur la virtualisation (VBS). La VBS isole les sites web et les documents Office non fiables des données utilisateurs et protège les zones clés, telles que les banques d'identifiants, en offrant une isolation au niveau matériel et en prévenant les attaques de type « pass-the-hash ». Cela aide à assurer la protection, y compris si le système d'exploitation est compromis.

Alors que le nombre total de vulnérabilités Windows a légèrement augmenté en 2022 (revenant à des niveaux proches de 2018), les vulnérabilités critiques Windows ont poursuivi leur tendance à la baisse depuis l'entrée en vigueur de ces changements. Nous nous attendons à ce qu'une tendance générale à la baisse se poursuive, même si les progrès se feront petit à petit puisqu'il reste beaucoup de code hérité du passé.



Vulnérabilités Microsoft Office (2017-2022)

■ Total des vulnérabilités
■ Vulnérabilités critiques



La suite Microsoft Office a fortement gagné en maturité au cours des dernières années, entraînant une baisse des vulnérabilités et supprimant des vecteurs d'attaque, mais leur atténuation ne s'est pas faite sans mal en 2022.

La catégorie des produits Microsoft Office a connu une baisse de 45 % des vulnérabilités en 2022, alors que les vulnérabilités critiques sont passées d'un minimum d'une en 2021 à deux instances en 2022.

Bien qu'il y ait une tendance générale à la baisse depuis cinq ans du nombre de vulnérabilités Microsoft Office, les applications Office ont continué d'être une cible de choix pour les acteurs malveillants. Cela est dû en grande partie au délai séparant la détection de la correction, comme démontré par les CVE-2022-30190 et CVE-2022-34713, toutes deux détaillées ci-dessous.

En plus de corriger les vulnérabilités, Microsoft s'est efforcé d'éliminer les vecteurs d'attaque courants, tels que les macros VBA dans les documents qui sont transmises à partir d'Internet. Il s'agit d'un vecteur d'attaque extrêmement fréquent, mais les tentatives précédentes pour y remédier consistaient simplement en des blocages logiciels qui étaient facilement contournés en incitant l'utilisateur final à activer des macros au moyen de stratagèmes d'ingénierie sociale.

En 2022, Microsoft a renforcé les protections contre ce vecteur d'attaque en bloquant par défaut les macros Internet dans les applications Office. Ce blocage ne s'est pas aussi bien passé que prévu. [Microsoft a annoncé cette démarche en février, a procédé au déploiement en avril et est temporairement revenu sur sa décision](#) avant de fournir durant l'été une autre mise à jour [permettant de bloquer par défaut les macros VBA](#) après avoir reçu des commentaires des utilisateurs. Cela a créé une confusion extrême.

Ainsi, bien que nous ayons vu les tendances concernant les vulnérabilités Microsoft Office évoluer dans la bonne direction, la mise en place de correctifs en 2022 n'a pas été sans heurts. Heureusement, nous constaterons à l'avenir une réduction du délai entre la détection et la correction.



Les vulnérabilités les plus marquantes de Microsoft Office

Le système CVE (Common Vulnerabilities and Exposures) fournit une méthode de référence pour les vulnérabilités et les risques de sécurité des informations connus publiquement.

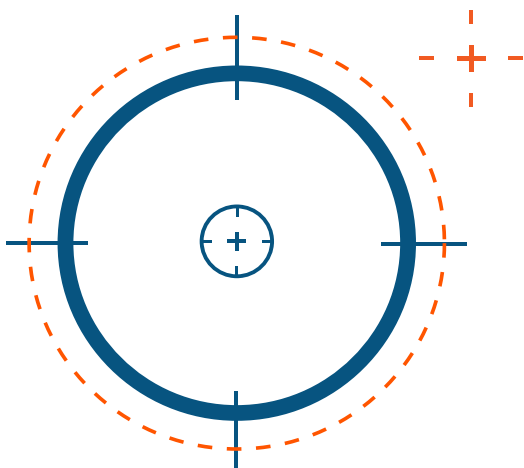
L'exploit Follina et la CVE-2022-30190

Score de base CVSS de 7,8 et score temporel de 7

Bien qu'il soit difficile de désigner la vulnérabilité la plus marquante, l'exploit « Follina » qui a mené à la vulnérabilité Office CVE-2022-30190 fut mémorable. C'était une faille zero-day qui rendait possible une exécution de code à distance dans les produits Office. Cette faille tirait notamment parti du protocole Microsoft Office et de MSDT, un outil d'assistance Microsoft utilisé pour permettre à un code de s'exécuter, même si les macros ont été désactivées ou lorsque l'utilisateur a simplement ouvert un aperçu du fichier. Follina fut rapidement exploité par des acteurs malveillants dans diverses campagnes d'attaque.

La chronologie de cette vulnérabilité et la réponse qui y a été apportée ont été particulièrement intéressantes. Dès 2021, des chercheurs [ont soulevé la question de l'utilisation abusive de protocoles Office](#), mais cette question a d'abord été considérée comme sans importance. Des rapports faisant état de l'utilisation de ces techniques ont commencé à apparaître en avril et en mai 2022. D'autres rapports furent transmis à Microsoft, mais il a fallu attendre le 30 mai pour qu'une CVE soit publiée. Un correctif fut enfin publié le 14 juin. À ce stade cependant, Qakbot et d'autres acteurs malveillants exploitaient activement la vulnérabilité.

Apprenez-en plus sur la faille Follina [ici](#)





DogWalk et la CVE-2022-34713

Score de base CVSS de 7,8 et score temporel de 7,2

À l'instar de Follina, [DogWalk \(CVE-2022-34713\)](#) exploitait également l'outil d'assistance MSDT de Microsoft. DogWalk a été signalé pour la première fois par Microsoft fin 2019, mais Microsoft [a initialement négligé](#) l'impact potentiel et l'importance de la vulnérabilité. Ce fut surprenant, étant donné que la vulnérabilité permettait à un attaquant de provoquer l'exécution d'un code en déposant un fichier exécutable dans un dossier de démarrage Windows lorsque la victime ouvrait un fichier diagcab.

Étant donné que les navigateurs ne considéraient pas les fichiers diagcab comme une menace, il était possible d'effectuer un téléchargement « Drive-by » et de déclencher la faille simplement en visitant un site web malveillant. Par la suite, cette faille fournissait un moyen de contourner la « marque du web », à savoir le marquage des fichiers comme provenant d'Internet et, par conséquent, l'indication d'un degré moindre de confiance (un aspect que surveillent de nombreuses solutions de sécurité). Enfin, DogWalk fournissait un moyen simple de provoquer une exécution et une persistance en lançant des charges utiles au démarrage.

Microsoft fit demi-tour uniquement après que des rapports aient fait état de l'exploitation « zero-day » de DogWalk en plus de nouvelles informations sur la vulnérabilité Follina. En août 2022, Microsoft a décidé de corriger cette vulnérabilité et a [publié une mise à jour de sécurité](#).

Quels enseignements tirer de DogWalk et de Follina ? L'importance de reconnaître et d'atténuer de manière proactive les vulnérabilités.

Bien que DogWalk ne soit pas à proprement parler une vulnérabilité d'Office, il vaut la peine d'être mis en évidence avec Follina car ils racontent tous deux l'histoire de la confusion qui règne lorsque des chercheurs divulguent des vulnérabilités, que Microsoft rejette dans un premier temps les résultats et que les clients se retrouvent pris au piège entre les deux.

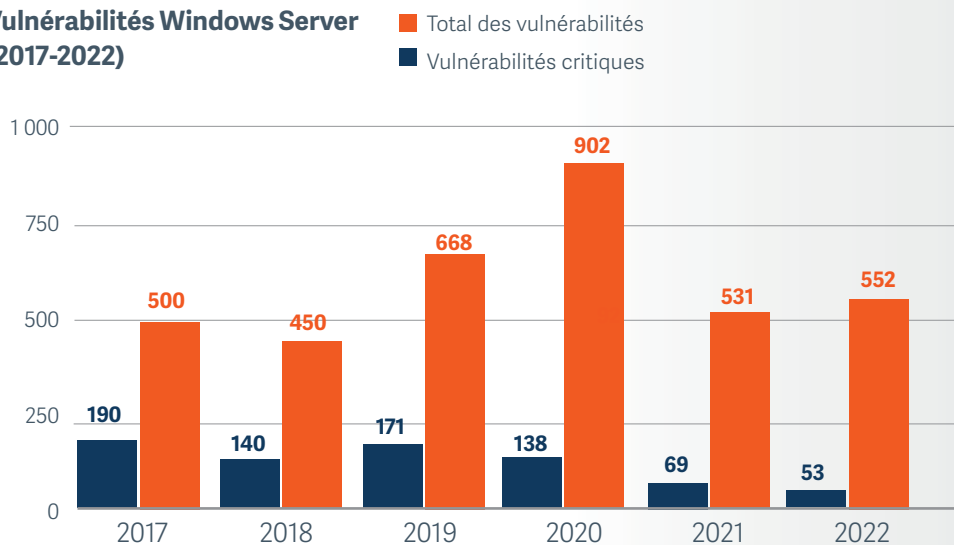
La frontière entre les vulnérabilités, les bugs et le « fonctionnement comme prévu » peut devenir très floue. Souvent, la détection de ce type de problèmes ne révèle que la partie émergée de l'iceberg.

Lorsque Microsoft décide dans un premier temps que quelque chose n'est pas une vulnérabilité, les chercheurs en sécurité et les acteurs malveillants commencent à tirer sur les fils pour voir ce qu'il est possible de démêler. Nous reviendrons sur ce point ultérieurement en parlant de l'« effet boule de neige des vulnérabilités ».

Le principal défi en la matière est de faire en sorte que les vulnérabilités ayant un impact soient reconnues comme telles plus tôt et corrigées plus rapidement, plutôt que de se baser sur des failles se répandant librement et la pression des réseaux sociaux pour mener le processus.



Vulnérabilités Windows Server (2017-2022)



La couverture des correctifs reste une préoccupation alors que les vulnérabilités totales et critiques Windows Server sont en baisse depuis 4 ans.

La catégorie Windows Server a connu une augmentation de 4 % du nombre total de vulnérabilités d'une année sur l'autre, tandis que son nombre de vulnérabilités critiques a poursuivi sa baisse de plusieurs années, chutant d'un pourcentage notable de 23 % par rapport à l'année précédente. Le nombre de vulnérabilités critiques Windows Server a diminué de 72 % depuis 2017, un chiffre impressionnant.

L'une des préoccupations concernant les vulnérabilités Windows Server est la couverture des correctifs. La [Shadowserver Foundation](#) a signalé que, fin décembre 2022, près de 70 000 implémentations de Microsoft Exchange Server n'étaient toujours pas protégées contre les vulnérabilités ProxyNotShell (CVE-2022-41040 et CVE-2022-41082) qui ont été découvertes en septembre 2022.

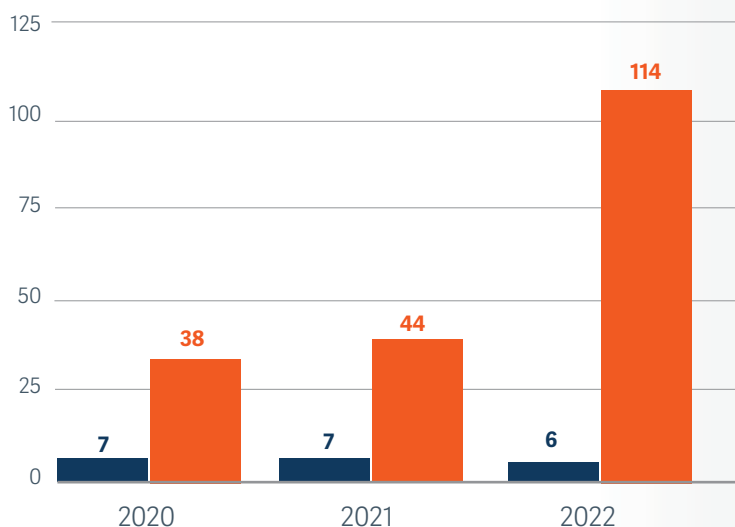
Comme pour les vulnérabilités du Windows Print Spooler (détaillées ci-dessous), ProxyNotShell a continué de provoquer des problèmes même après que ses vulnérabilités aient été corrigées. En décembre 2022, des chercheurs de [CrowdStrike ont découvert « OWASSRF »](#), une méthode de contournement des mesures d'atténuation mises en place par Microsoft. La faille OWASSRF a été utilisée par un certain nombre de pirates utilisant du ransomware, y compris lors des attaques contre H-Hotels et Rackspace.

La situation a généré une certaine controverse. Par exemple, certaines organisations [se sont prétendument abstenues d'appliquer des correctifs](#) en raison de rapports faisant état d'erreurs d'authentification qui auraient pu entraîner des temps d'arrêt, et de préoccupations selon lesquelles le correctif aurait de toute façon pu être contourné. Le choix cornélien entre assurer le fonctionnement continu des serveurs et garantir leur sécurité peut donner des sueurs froides aux décideurs IT.



Vulnérabilités Azure et Dynamics 365 (2020-2022)

■ Total des vulnérabilités
■ Vulnérabilités critiques



Microsoft Azure et Dynamics 365 ont connu la plus forte augmentation de vulnérabilités parmi toutes les catégories de produits Microsoft en 2022, passant de 44 en 2021 à 114 l'année dernière, soit une augmentation de 159 %.

Étant donné la large gamme de produits couverts par Microsoft Azure et Dynamics 365, cette augmentation ne serait pas très surprenante. Un outil spécifique semble toutefois avoir représenté la majorité des occurrences croissantes de cette vulnérabilité.

L'outil Azure Site Recovery VMware a généré à lui seul 80 vulnérabilités en 2022. Cette suite fait partie du service de reprise après sinistre qui peut automatiquement basculer des workloads vers un site secondaire lorsqu'un problème est détecté. Il est donc à la fois préoccupant et rassurant de constater qu'un nombre si important de vulnérabilités ait été corrigé.

La majorité des vulnérabilités d'Azure Site Recovery ont été classées dans la catégorie Élévation de privilèges et semblent partager une cause initiale : une injection SQL (SQLi). Le fait que SQLi ait figuré dans la [liste du Top 10 de l'OWASP](#), qui recense les problèmes les plus fréquents concernant la sécurité des applications en ligne, sert à nous rappeler utilement que nous devons tirer des enseignements du passé.



L'effet boule de neige des vulnérabilités

Nous essayons chaque année de répondre à la question : **que signifient les tendances ?** Parfois, une telle réponse se rapporte autant à la nature humaine qu'à n'importe quel motif technique.

Nous savons que l'écosystème Microsoft est vaste et offre une surface d'attaque potentielle qui ne cesse de croître.

Bien que la plupart du code nouvellement ajouté soit créé selon des pratiques de développement sécurisées et soit moins susceptible d'introduire de nouvelles vulnérabilités que les années précédentes, le code hérité sur lequel repose l'écosystème continue d'occuper une place importante.

Dans le cas des systèmes d'exploitation Windows, chaque version a été une évolution de la précédente et non une réécriture totale. Cela signifie que le noyau Windows NT a fortement évolué depuis 1993, il a aussi conservé une grande part de son code initial.

C'est là où intervient la nature humaine. Les chercheurs tombent de temps à autre sur un aspect qui s'avère être une mine d'or de vulnérabilités. Une vulnérabilité est trouvée et corrigée, mais au cours du processus, l'attention est attirée par quelque chose qui n'avait pas été noté antérieurement. D'autres chercheurs s'y intéressent et trouvent de nouvelles vulnérabilités, de nouveaux vecteurs d'attaque et de nouvelles façons de contourner les correctifs précédents. C'est alors que le nombre de vulnérabilités commence à avoir un effet boule de neige.

L'effet boule de neige des vulnérabilités en action : Le service Print Spooler

Le service Print Spooler contient un vieux code de plus de 20 ans et constitue un exemple clair de la façon dont une vulnérabilité peut continuer à causer des problèmes, même lorsqu'elle est corrigée.

2018

« Le bug de l'imprimante » est identifié. Ce bug permet à un utilisateur ne disposant pas de privilèges dans le réseau de déclencher à distance le service Print Spooler du contrôleur de domaine pour s'authentifier auprès d'un système quelconque. Ce bug permet à l'attaquant de se faire passer pour le contrôleur de domaine.

2019

« Le bug de l'imprimante » devient [CVE-2019-0683](#) et attire l'attention sur le service Print Spooler.

2020

Sept (7) vulnérabilités liées à l'élévation de privilèges et au Windows Print Spooler sont divulguées. Ces vulnérabilités sont toutes initialement des vecteurs d'attaque locale, obligeant l'attaquant à d'abord avoir un accès direct au système exécutant le Print Spooler. Cependant, le résultat de chacune d'elles est qu'un attaquant pourrait exécuter un code de son choix avec des privilèges système élevés.

[CVE-2020-1030](#)

[CVE-2020-1048](#)

[CVE-2020-1070](#)

[CVE-2020-1337](#)

[CVE-2020-17001](#)

[CVE-2020-17014](#)

[CVE-2020-17042](#)

Apparaît vers la fin 2020. À la différence des failles précédentes qui étaient exploitables localement, celle-ci peut l'être à distance, ce qui signifie que l'attaquant doit seulement être présent sur le réseau. Cet attribut RCE (exécution de code à distance) rend cette vulnérabilité spécifique bien plus grave. Cependant, cette vulnérabilité n'a pas été divulguée publiquement et on suppose qu'elle n'a pas été exploitée librement avant d'être corrigée.



2021

16 vulnérabilités liées à l'élévation de privilèges et au Windows Print Spooler sont divulguées. Le Print Spooler attire désormais l'attention de nombreux chercheurs en tant que moyen d'effectuer des attaques avec une élévation de privilèges. Le nombre de vulnérabilités divulguées relatives à l'élévation de privilèges dans le contexte du Windows Print Spooler augmente rapidement alors que Microsoft joue au jeu de la taupe avec les chercheurs ayant trouvé des moyens de contourner les correctifs et de continuer à exploiter les vulnérabilités.

[CVE-2021-34527](#) est la plus notable des vulnérabilités dans la catégorie 2021 de l'élévation de privilèges et du Windows Print Spooler. Cette vulnérabilité est très simple à exploiter. Un réseau n'avait besoin que d'un compte utilisateur valide et du Print Spooler pour autoriser les connexions à distance (qui sont activées par défaut). La facilité de la faille, combinée au fait qu'elle ait été divulguée publiquement et ait été activement et librement utilisée, lui a valu le nom de « cauchemar d'impression ».

Les 15 autres vulnérabilités similaires de la promotion 2021

comprennent : CVE-2021-41333, CVE-2021-41332, CVE-2021-40447, CVE-2021-38671, CVE-2021-38667, CVE-2021-36970, CVE-2021-36958, CVE-2021-36947, CVE-2021-36936, CVE-2021-34483, CVE-2021-34481, CVE-2021-26878, CVE-2021-1695, CVE-2021-1675 et CVE-2021-1640.

2022

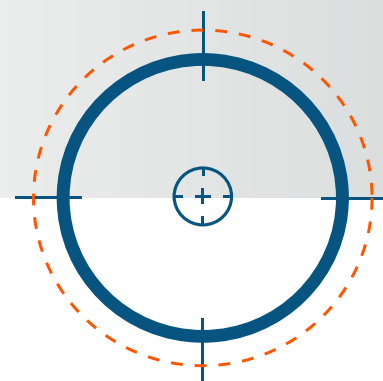
35 vulnérabilités liées à l'élévation de privilèges et au Windows Print Spooler sont divulguées, soit plus du double par rapport à l'année précédente.

CVE-2022-44681, CVE-2022-44678, CVE-2022-41073, CVE-2022-38028, CVE-2022-38005, CVE-2022-35793, CVE-2022-30226, CVE-2022-30206, CVE-2022-30138, CVE-2022-29140, CVE-2022-29132, CVE-2022-29114, CVE-2022-29104, CVE-2022-26803, CVE-2022-26802, CVE-2022-26801, CVE-2022-26798, CVE-2022-26797, CVE-2022-26796, CVE-2022-26795, CVE-2022-26794, CVE-2022-26793, CVE-2022-26792, CVE-2022-26791, CVE-2022-26790, CVE-2022-26789, CVE-2022-26787, CVE-2022-26786, CVE-2022-23284, CVE-2022-22718, CVE-2022-22717, CVE-2022-22041, CVE-2022-22022, CVE-2022-21999 et CVE-2022-21997

Quels enseignements pouvons-nous en tirer ? Comme le dit le proverbe, « Il n'y a pas de fumée sans feu ».

Soyez vigilants face à ces menaces émergentes, de façon à prendre des décisions mieux avisées. Par exemple, si vous avez constaté une tendance à la hausse des vulnérabilités associées au Windows Print Spooler, vous n'aurez peut-être pas empêché une attaque de type "zero-day", mais vous aurez au moins pu comprendre votre exposition et les mesures d'atténuation potentielles.

Le service Print Spooler aurait pu être désactivé lorsqu'il n'était pas nécessaire, la recherche des systèmes exposés aurait été faite et les paramètres et les contrôles auraient été appliqués afin d'en modifier le comportement. Rien de cela n'empêche les vulnérabilités ni leur détection mais cela permet à votre organisation de mieux se protéger, ainsi que ses clients et partenaires.





Qu'en dit ChatGPT ?

ChatGPT, un agent conversationnel utilisant l'intelligence artificielle, a été sur toutes les lèvres dans le secteur de la technologie en 2022 et ce jusqu'à aujourd'hui. La prochaine génération d'agents conversationnels utilisant l'intelligence artificielle a le potentiel de tout révolutionner, depuis les devoirs de vos enfants jusqu'aux réponses en cas d'incident informatique.

Microsoft a fortement investi depuis 2019 dans OpenAI, le développeur de ChatGPT et dispose de plans ambitieux pour intégrer l'IA dans un certain nombre de ses produits. ChatGPT est déjà en train d'être intégré dans Bing, le moteur de recherche de Microsoft, dans l'espoir d'en faire un rival plus sérieux de Google, bien que nous ne soyons pas convaincus que les expressions « Tiens, je vais binger ça pour toi » ou « As-tu essayé de binger la réponse » deviennent communes en 2023.

Quel sera l'impact du développement de l'IA sur le paysage et les rapports en matière de vulnérabilités ? Avant d'aborder nos commentaires d'experts en cybersécurité, nous avons pensé qu'il serait utile et opportun de poser quelques questions à ChatGPT.



What do you think about the Microsoft Vulnerabilities report by BeyondTrust?



As an AI language model, I do not have personal opinions. However, I can provide information and context about the Microsoft Vulnerabilities report by BeyondTrust that you mentioned.



The Microsoft Vulnerabilities report by BeyondTrust is an annual report that provides information about the state of security for Microsoft products and services. The report typically includes data on the number and types of vulnerabilities discovered in Microsoft products, as well as trends and insights into the state of security for Microsoft products.

Reports like this can be valuable for organizations that use Microsoft products and services, as they provide a snapshot of the current state of security and can help organizations prioritize their security efforts. However, it's important to keep in mind that the information in these reports is subject to change and should be considered in the context of a larger security strategy.

Additionally, it's important for organizations to stay informed about security threats and best practices for protecting their systems, regardless of the specific products and services they use. This can include regular security audits, software updates and patches, and ongoing education and training for employees.



S'agissant des vulnérabilités, l'un des défis généraux de l'intelligence artificielle et de l'apprentissage machine est la transparence et l'explicabilité des modèles utilisés. Cela signifie que non seulement **l'IA pourrait introduire de toutes nouvelles catégories de vulnérabilités**, mais que les vulnérabilités pourraient également être encore **plus difficiles à détecter et à corriger**.

Les vulnérabilités liées à l'IA sont généralement différentes des bugs traditionnels figurant dans un code pouvant être corrigés en déterminant la ou les lignes du code en question. L'IA apprend à partir d'ensembles de données parfois gigantesques et accroît essentiellement le nombre d'entités pouvant être utilisées pour exploiter un système.

Si l'on considère que les informations erronées diffusées en ligne et consommées par l'IA pourraient conduire à des réponses et à des décisions dangereuses, on commence à voir où les problèmes pourraient émerger. Nous pouvons également penser à des objets physiques, comme un panneau d'arrêt « STOP » en carton dessiné à la main qui provoque l'arrêt de votre voiture lorsque l'IA du véhicule le confond avec un véritable panneau d'arrêt.



Will AI introduce a new class of security vulnerabilities?



Yes, it is possible that artificial intelligence (AI) will introduce new security vulnerabilities. As AI systems become more widespread and integrated into critical infrastructure, their potential for harm also increases. Additionally, AI systems can be vulnerable to manipulation and exploitation by malicious actors, who could use AI to carry out cyber attacks or gain unauthorized access to sensitive information.



For example, AI systems that rely on machine learning algorithms can be vulnerable to adversarial attacks, in which attackers manipulate input data to cause the AI system to behave in unexpected or harmful ways. AI systems that process sensitive information may also be vulnerable to data breaches, as attackers seek to steal valuable information or manipulate AI systems for their own gain.

It is important for organizations to be proactive in addressing the potential security risks posed by AI, by incorporating security measures into the design and implementation of AI systems and by staying informed about emerging threats and best practices for protecting AI systems.



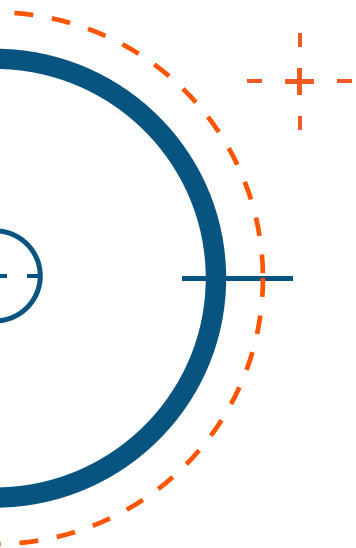
Une étude de 2022 intitulée [« Les utilisateurs rédigent-ils des codes moins sûrs en utilisant des assistants optimisés par IA ? »](#) a révélé que des chercheurs de Stanford ont constaté que les développeurs utilisant de tels assistants pour écrire un code sont plus susceptibles d'introduire des vulnérabilités de sécurité.

De même, les conclusions de ces chercheurs indiquent que les utilisateurs d'assistants à base d'IA sont plus enclins à croire qu'ils rédigent un code mieux sécurisé que leurs pairs n'utilisant pas d'IA.

Les chercheurs de Stanford ont déclaré : « Nous avons constaté que les participants ayant accès à un assistant à base d'IA génèrent souvent plus de failles de sécurité que ceux qui n'y avaient pas accès, avec des résultats particulièrement significatifs pour le chiffrement de chaîne et l'injection SQL. »

Bien que la portée de l'étude de Stanford fut limitée, celle-ci a fourni de précieux renseignements concernant les risques cachés de l'IA : **sa capacité à introduire un risque tout en réduisant notre perception du risque.**

À mesure que Microsoft ajoutera des capacités d'IA dans ses produits, il sera intéressant de constater quel en sera l'impact sur la quantité et la gravité des vulnérabilités publiées. Après avoir fait des progrès si significatifs en matière de sécurité depuis le fameux [Trustworthy Computing Memo rédigé en 2002 par Bill Gates](#), nous ne pouvons qu'espérer que [les propos plus récents du fondateur de Microsoft](#) comparant l'IA à l'énergie nucléaire - « toutes deux prometteuses et dangereuses » - ne passent pas inaperçus.





Qu'en disent les experts ?

Jane Frankland

CEO, KnewStart
Fondatrice, IN Security Movement

Derek Hanson

Vice President Solutions
Architecture & Alliances, Yubico

Charles Henderson

Global Managing Partner,
Directeur de X-Force, IBM

Troy Hunt

Fondateur et PDG, Have I Been Pwned,
Microsoft Regional Director & MVP

Paula Januszkiewicz

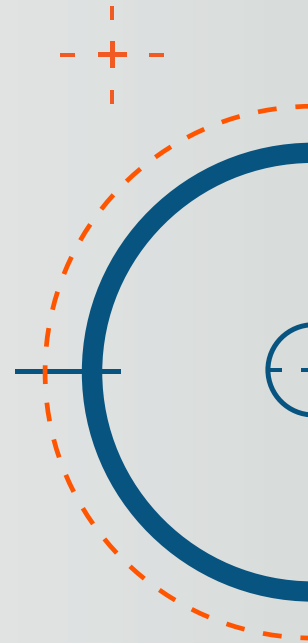
PDG, CQURE

Marc Maiffret

Chief Technology Officer, BeyondTrust

Avi Shua

PDG et cofondateur, Orca Security





LinkedIn | Twitter

Jane Frankland

CEO, KnewStart

Fondatrice, IN Security Movement



COMMENTAIRE

La cybersécurité est un secteur en constante évolution, avec de nouvelles menaces et technologies qui apparaissent chaque jour et font souvent la une des médias. L'an dernier, nous avons vu des cyberdélinquants profiter des pratiques du télétravail - qui découlent directement de la pandémie de Covid 19 - pour lancer des attaques sans précédent contre des réseaux d'entreprises dans le monde entier.

En outre, alors que les deepfakes, les e-mails de phishing générés par IA et d'autres méthodes sophistiquées d'ingénierie sociale deviennent moins coûteux et plus fréquents, nous constatons qu'un nombre croissant de personnes ont du mal à se protéger contre les violations de données et les manquements en matière de conformité.

Le Microsoft Vulnerabilities Report de BeyondTrust met en évidence le fait que les vulnérabilités Microsoft continuent d'augmenter année après année, et que les pirates continuent d'utiliser le vol d'identité comme vecteur d'attaque - avec un nombre croissant d'exécutions de codes à distance et d'élévations de privilèges pour atteindre leurs cibles. Toutefois, cela révèle aussi que le nombre de vulnérabilités critiques utilisées par ces attaques diminue.

Les vulnérabilités critiques ayant atteint leur plus bas niveau depuis dix ans, le rapport suggère qu'une attaque réussie nécessite désormais des compétences et des outils plus sophistiqués, ce qui pourrait réduire le nombre d'attaquants potentiels.

C'est une nouvelle formidable. Microsoft a investi beaucoup de ressources pour améliorer la sécurité au fil des ans, et cela porte ses fruits.

De nombreux produits Microsoft sont disponibles dans des versions à long terme, ce qui permet aux organisations de passer en toute sécurité à des produits plus récents et plus sûrs et à des instances SaaS où tout le monde reste à jour.

Compte tenu du paysage actuel des menaces et des informations contenues dans le rapport de BeyondTrust, les responsables sécurité seraient avisés d'appliquer, à l'horizon 2023, le principe du moindre privilège et de surveiller l'accès aux identités pour renforcer la protection contre les menaces futures, notamment la perte de revenus, de propriété intellectuelle, de réputation et les amendes. Ils peuvent aussi garder une longueur d'avance en passant de méthodes d'authentification multi-facteurs (MFA) moins efficaces, comme les SMS et les applications mobiles, à des authentificateurs matériels d'une qualité supérieure, par exemple l'authentification FIDO pour une protection renforcée contre le phishing.

Cette approche doit être combinée avec d'autres pratiques exemplaires, comme l'intégration de la sécurité dans les priorités commerciales, la sensibilisation à la sécurité chez les employés et les fournisseurs, la mise à jour des logiciels au moyen des derniers correctifs de sécurité, la surveillance du réseau pour détecter une activité suspecte, l'application d'un programme de gestion des vulnérabilités efficace, ainsi que la disponibilité d'un plan de réponse aux incidents bien préparé et la sauvegarde des données.



[LinkedIn](#) | [Twitter](#) | [Site Web](#)

Derek Hanson

Vice President

Solutions Architecture & Alliances

Yubico



COMMENTAIRE

Tout comme les cyberattaques ont augmenté à l'échelle mondiale, Microsoft a constaté une hausse frappante des vulnérabilités. L'analyse des tendances sur 10 ans contenue dans ce rapport procure des renseignements uniques et utiles pour les professionnels de la sécurité cherchant à protéger leur organisation des menaces actuelles et futures. Examinons tout d'abord les menaces actuelles.

Obtenir un accès admin aux systèmes utilisateur a toujours été comme décrocher le jackpot pour les attaquants. Le préjudice causé par l'accès à un seul compte privilégié est catastrophique pour de nombreuses organisations et est à l'origine d'un nombre croissant de violations de données qui font la une des médias. Comme le montre ce rapport, il est essentiel que les organisations appliquent le principe du moindre privilège et suppriment les droits admins inutiles pour atténuer proactivement les vulnérabilités.

À quoi ressembleront les futures menaces ? Comme l'avait indiqué William Gibson, « Le futur est là, mais il n'est pas encore largement distribué ». Nous sommes témoins d'une évolution de l'apprentissage machine et de l'intelligence artificielle qui se déroule maintenant, sous nos yeux. Ces technologies commencent à être employées pour créer des « deep fakes » des voix et des visages dignes d'une dystopie. Elles sont en mesure de créer des répliques synthétiques des caractéristiques qui peuvent être validées par de nombreuses solutions biométriques au cours d'une authentification.

L'impact de la technologie des deep fakes sur les solutions d'authentification à base de biométrie augmentera à mesure qu'elle deviendra plus accessible et plus facile

à utiliser. Les solutions qui s'appuient sur une technologie biométrique à distance pour valider des identités devront évoluer pour détecter cette technologie ou seront distancées. Aujourd'hui, et par la suite pour assurer une protection avancée, les solutions biométriques doivent être soutenues par des authentificateurs matériels modernes, tels que des clés de sécurité, qui fonctionnent sur toutes les plateformes et sécurisent davantage ces options.

Pour résumer, il est impératif que les organisations s'attaquent aux menaces actuelles en mettant en place des stratégies telles que le moindre privilège et le contrôle d'accès aux identités afin de réduire le risque (si le pire devait se produire). Il est également essentiel que les professionnels de la sécurité gardent une longueur d'avance et délaissent les méthodes d'authentification multi-facteurs (MFA) existantes, telles que les SMS et les applications mobiles, pour se reporter sur des authentificateurs portables et matériels basés sur une authentification FIDO offrant des capacités de résistance au phishing visant la MFA.

Nous vivons peut-être dans un monde où la frontière entre science-fiction et réalité commence à s'estomper, mais dans cette course rapide aux armements, nous disposons déjà de solutions d'authentification hautement efficaces résistant au phishing - et de solutions de gestion des accès privilégiés - qui nous fournissent la sécurité mesurable et fiable dont nous avons besoin.

[LinkedIn](#) | [Twitter](#)

Charles Henderson

Global Managing Partner, Directeur de X-Force IBM



COMMENTAIRE

Dans le paysage actuel des cybermenaces, les entreprises font face au défi impossible de localiser chaque vulnérabilité en raison du volume considérable de celles qui sont divulguées chaque année. Bien que des exploits puissent toujours entraîner des incidents majeurs, les vulnérabilités et les exploits ne requièrent pas tous la même attention. Les attaquants tendent à se concentrer sur les vulnérabilités et les exploits qui fonctionnent pour leurs opérations, et l'intégration d'un nouvel exploit ou d'une nouvelle vulnérabilité requiert une nouvelle façon d'attaquer et des investissements supplémentaires.

Le Microsoft Vulnerabilities Report de BeyondTrust illustre la hausse préoccupante des vulnérabilités. Il faut ajouter à cela le temps et les ressources nécessaires pour apporter un correctif ou trouver une solution de contournement. Il n'est donc pas surprenant que les entreprises considèrent qu'il est de plus en plus difficile de suivre les pratiques de gestion des vulnérabilités. Se concentrer sur les correctifs uniquement n'est plus faisable. Les cyberdélinquants ont accès à des milliers d'exploits, et la cybercommunauté continue d'être en proie à une pénurie de talents et de ressources financières qui sont utilisées au maximum de leurs possibilités.

Les entreprises doivent donner la priorité aux programmes de gestion des vulnérabilités basés sur les menaces et à la mise en œuvre du principe du moindre privilège pour réduire les risques. En comprenant la façon dont les attaquants opèrent et tirent parti de l'exploitation des vulnérabilités pour atteindre leurs objectifs, les entreprises peuvent donner la priorité à leurs efforts de gestion des vulnérabilités basée sur le risque et sur l'impact potentiel pour leur activité. Cela se traduit par une liste des vulnérabilités bien plus gérable.

La même approche basée sur les menaces peut être

étendue à la manière dont les organisations envisagent les exploits de type zero-day. Bien que les exploits zero-day fassent souvent la une des médias, l'analyse des tendances en matière de vulnérabilité montre que la découverte d'un zero-day est bien peu de chose au regard du nombre de vulnérabilités existantes, les organisations étant incapables de suivre le rythme des correctifs.

L'analyse de la base de données cumulative de X-Force sur les vulnérabilités et les exploits montre que, même si la découverte de vulnérabilités a rapidement augmenté d'une année sur l'autre, seulement 3 % d'entre elles étaient associées à un zero-day. En outre, l'analyse des comportements des attaquants révèle que ceux-ci préfèrent exploiter des vulnérabilités anciennes et connues plutôt que de découvrir ou de tirer parti des exploits zero-day les plus récents et les plus spectaculaires.

En 2022, WannaCry (tirant parti d'une vulnérabilité de 2017) était la variante de ransomware qui se classait au deuxième rang en ce qui concerne la fréquence, comme l'a observé X-Force. La gestion des vulnérabilités basée sur les menaces permet aux organisations de sortir du cercle vicieux des vulnérabilités et du zero-day et de progresser véritablement s'agissant de la réduction des risques en ciblant leurs efforts sur les vulnérabilités les plus susceptibles d'être exploitées par les attaquants et d'avoir les plus fortes conséquences sur leur activité. Concernant la masse restante de vulnérabilités et d'exploits, les entreprises doivent affecter des ressources pour détecter et réagir aux comportements qui indiquent une exploitation, nonobstant la vulnérabilité utilisée.

En améliorant leurs capacités de détection et de réaction, les entreprises peuvent compliquer la tâche des attaquants, même s'ils parviennent à obtenir un accès par l'exploitation d'une vulnérabilité.



[LinkedIn](#) | [Twitter](#) | [Site Web](#)

Troy Hunt

Fondateur et PDG, Have I Been Pwned, Microsoft Regional Director & MVP



COMMENTAIRE

J'ai récemment été invité à la conférence annuelle de l'Association des fonds de pension australiens où j'ai pu aborder la cybersécurité devant un public composé de professionnels de la finance.

Il aurait été peu probable que je sois invité, ne serait-ce que six mois avant, mais deux violations massives de données se sont produites dans ce pays (une dans une entreprise de télécommunications de premier plan, l'autre chez l'une des plus importantes entreprises d'assurance santé privée), chacune révélant des renseignements sur près de la moitié de la population, ce qui a éveillé la curiosité du public et des conseils d'administration.

Ainsi, j'ai pu parler à ce public de professionnels de la finance d'un sujet peu familier pour la plupart d'entre eux, mais qu'ils avaient tous à l'esprit. Il était impossible de ne pas penser à la cybersécurité, au regard de son omniprésence dans les nouvelles pendant des mois, un aspect qui à lui seul vaut d'être noté. La cybersécurité est aujourd'hui un sujet d'actualité dont tout le monde est conscient, soit parce qu'il a été directement touché (je suis moi-même impliqué dans des dizaines de violations de données... à ma connaissance), soit parce que les médias en parlent sans cesse, soit parce que c'est devenu un sujet de discussion courant dans les réunions informelles.

La question de l'IA a inévitablement été soulevée durant l'événement -« **L'IA sera-t-elle utile ?** »- ce qui appelle une réponse évidente : **oui**.

Ce qui est moins évident au sujet de l'IA est à qui sera-t-elle utile. Bien que les projecteurs illuminant la scène m'empêchaient de voir précisément les réactions du public, il était évident que la plupart des personnes n'avaient pas réalisé que l'IA pourrait être utile à des personnes mal intentionnées.

Cela nous amène au sujet de la neutralité morale de la technologie. Tout comme le cryptage est bénéfique pour effectuer un paiement en ligne en toute sécurité autant que pour le crime organisé, l'IA profite également aux deux parties.

Je pourrais présenter les choses ainsi : à quel point un e-mail de phishing semblerait plus légitime s'il était écrit par ChatGPT plutôt que par un escroc ? C'est là toute la question !

Tout ceci dresse un paysage fascinant dans le domaine de la sécurité des informations. Chaque partie progresse rapidement vers ses objectifs respectifs sous le regard d'un nombre sans précédent de spectateurs qui deviennent souvent des acteurs involontaires dans la délinquance numérique.



Paula Januskiewicz

PDG

CQURE



COMMENTAIRE

Au cours de l'année passée, j'ai observé des événements de cybersécurité qui ont affecté des millions de personnes dans le monde entier. Les infrastructures d'entreprise sont désormais exposées aux nouveaux vecteurs d'attaque et aux nouvelles menaces.

Cependant, outre les dangers liés au télétravail, les années 2020 sont marquées par des attaques plus rapides : deepfakes en évolution rapide, e-mails de phishing avancé générés par l'IA et autres actions d'ingénierie sociale plus sophistiquées. Nous pouvons nous attendre à ce que les cybermenaces continuent d'évoluer et d'augmenter en 2023.

Grâce au Microsoft Vulnerabilities Report publié par BeyondTrust, nous sommes en mesure de conclure que les objectifs des hackers restent les mêmes, en mettant l'accent sur l'exécution de code à distance et l'élévation des privilèges. Chaque attaque se produit en utilisant une identité qui a des privilèges plus ou moins élevés et implique l'exécution de malwares, qu'il s'agisse d'un script, d'un exécutable, d'une injection de processus ou juste de moyens simples utilisés par les hackers pour effectuer du phishing.

Les vecteurs d'attaque malveillants, y compris l'IA et les deepfakes, utilisés pour communiquer avec une cible, ont changé. Pourtant, quel que soit le point d'entrée, même le plus simple, une cyberattaque réussie peut entraîner de lourdes pertes financières et la divulgation d'informations confidentielles.

C'est pourquoi il est fortement recommandé d'effectuer régulièrement des examens de stratégie de la cybersécurité et divers types de tests d'intrusion, car ils constituent l'un des moyens les plus efficaces d'identifier les vulnérabilités techniques de l'infrastructure IT de l'entreprise avant qu'une attaque ne se produise. J'estime que des audits et des efforts constants pour améliorer la sécurité sont des signes distinctifs qui caractérisent les organisations dotées de politiques matures en matière de cybersécurité.

Je trouve cependant prometteur que les vulnérabilités critiques de Microsoft aient atteint leur plus faible niveau sur la décennie couverte par les différents Microsoft Vulnerabilities Reports. Cela signifie en théorie que la réussite d'une attaque requiert un plus haut degré de compétences et d'outils de la part du hacker, de sorte que le nombre d'adversaires potentiels devrait être réduit.

À la lecture de la dernière édition du Microsoft Vulnerabilities Report, je m'attends à ce que 2023 voit naître un débat sur la préparation des réponses aux incidents. Toutes les organisations devraient réviser leurs objectifs de sécurité et préparer des plans de réponse aux incidents clairement rédigés et ayant fait l'objet de tests dûment exécutés. D'autres aspects critiques incluent la surveillance, ainsi que l'accès privilégié et la gestion des identités. La première chose nécessaire à un acteur malveillant lorsque l'attaque se déclenche est une identité. Par conséquent, il est impossible de créer un écosystème sûr sans revoir notre approche d'entreprise, encore et encore.



[LinkedIn](#) | [Twitter](#) | [Site Web](#)

Marc Maiffret

Chief Technology Officer BeyondTrust



COMMENTAIRE

En tant que CTO de BeyondTrust, et attirant l'attention depuis fort longtemps sur les vulnérabilités Microsoft, il est gratifiant de voir ce rapport fêter son dixième anniversaire et continuer à souligner le besoin de continuer à améliorer la sécurité chez Microsoft.

Au début des années 2000, j'ai constitué des équipes de recherche en sécurité en ayant pour but d'inciter Microsoft et d'autres entreprises à faire de la sécurité une priorité. Depuis lors, Microsoft a fait des progrès considérables dans l'amélioration de ses codes et de ses systèmes. La présence des vulnérabilités reste claire et celles-ci atteignent des valeurs records comme le souligne le rapport de cette année, mais nous constatons aussi que les investissements de Microsoft dans la sécurité ont porté leurs fruits, avec un nombre de vulnérabilités critiques en baisse comme jamais auparavant.

Au vu des changements intervenus au cours de la dernière décennie, on constate que la sécurité n'est plus considérée comme un ajout externe au système d'exploitation mais comme quelque chose qui doit être intégré. Il existe de nombreux exemples techniques de cela dans les dernières générations de Windows OS, qui sont bien plus résistantes et sécurisées par défaut. Ces changements apportés à l'architecture comptent pour beaucoup dans la réduction du nombre de vulnérabilités critiques.

Mais nous ne devrions pas trop baisser notre garde.

Il existe toujours une myriade de vulnérabilités à découvrir. La série de vulnérabilités du service de spooler d'impression découvertes au cours de l'année 2022 montre que le « cauchemar de l'impression » de Microsoft, qui a commencé en 2021, n'est pas encore terminé. À part cela, il existe de nombreuses vulnérabilités non découvertes, certaines vieilles de plusieurs décennies, résidant au sein des environnements Microsoft en attendant que des chercheurs ou des acteurs de la menace les découvrent.

Un aspect que ce rapport a si bien mis en évidence au fil des ans est que les correctifs et le concept intemporel du moindre privilège sont essentiels pour atténuer les risques auxquels font face les organisations. L'exécution de code à distance (RCE) demeurant l'une des principales catégories de vulnérabilités au cours de la décennie passée, nous devons nous assurer d'appliquer le principe du moindre privilège partout où nous avons des données, que ce soit sur site, sous forme hybride ou dans le cloud, afin de garantir que les exploits RCE ne confèrent pas des privilèges excessifs à un attaquant. Il est essentiel de créer les obstacles sur lesquels butera un attaquant s'il tente d'exploiter un zero-day ou une vulnérabilité connue.

Protégez-vous !

Marc



LinkedIn | Site Web

Avi Shua

PDG et cofondateur Orca Security



COMMENTAIRE

Les vulnérabilités restent le vecteur d'attaque le plus important dans le cloud et les conclusions du Microsoft Vulnerabilities Report de cette année réaffirment ce point de façon spectaculaire. Avec l'énorme augmentation de 159 % des vulnérabilités dans Azure et Dynamics 365, les entreprises doivent être plus vigilantes que jamais en ce qui concerne les stratégies de sécurité et d'application de correctifs. Une grande partie de l'atténuation des risques commence par l'application du moindre privilège. Cela a été une étape importante pendant de nombreuses années (et l'est toujours) en ce qui concerne les systèmes cloud et les appareils de l'IoT.

Peut-être maintenant plus que jamais, les organisations comprennent le besoin essentiel de hiérarchiser les problèmes sur la base de leur zone d'effet potentielle et de l'impact commercial d'un risque. Cela ne peut être réalisé que lorsqu'une organisation dispose d'une ample visibilité et de renseignements contextuels se rapportant à son environnement. Comme le montre ce rapport, les vulnérabilités critiques comportent des niveaux de menace et un impact contextuels, en particulier compte tenu du système unique de notation de la gravité de Microsoft.

Je vais illustrer ce point avec l'exemple suivant : Les serveurs 1 et 2 sont des serveurs web utilisant une bibliothèque vulnérable (CVE-2018-1176). Sans mise en contexte, les risques pesant sur chacun des serveurs semblent être les mêmes. Cependant, en accédant à des données contextuelles, nous constatons que le serveur 1 est connecté à Internet et est facilement accessible par les attaquants.

En outre, le serveur 1 expose une clé pour accéder à

des ressources adjacentes contenant des informations personnellement identifiables. Par conséquent, la CVE du serveur 1 devrait être classée comme un risque élevé. D'autre part, le serveur 2 est un serveur intranet qui n'est pas accessible au public et n'expose aucun autre risque exploitable. Sa CVE présente donc un risque minimal et devrait être classée comme informationnelle uniquement.

Dans le [Public Cloud Security Report](#) de l'an dernier, 78 % des chemins d'attaque identifiés reposaient sur des vulnérabilités connues (les CVE) en tant que vecteur d'attaque initial pour obtenir un accès et, en moyenne, ne nécessitaient que trois étapes pour atteindre les données des « joyaux de la couronne ». Fort heureusement, la plupart des points d'entrée des attaquants peuvent être anticipés relativement facilement puisque ces CVE sont connues. La majorité disposent de moyens d'atténuation et, généralement, seul un pourcentage très faible d'entre eux sont exposés en externe. La diminution du risque est encore plus importante lorsque les droits d'administrateur sont supprimés et lorsque les identités sont sécurisées de façon efficace.

En s'appuyant sur des renseignements contextuels et en hiérarchisant efficacement les risques, les équipes de la sécurité dans le cloud peuvent appliquer des atténuations de façon stratégique, corriger en premier les risques les plus dangereux et travailler plus intelligemment, et non plus intensément. De plus, en prenant des mesures préventives pour réduire la capacité d'un attaquant à se déplacer latéralement, par exemple en contrôlant les accès privilégiés, les organisations peuvent s'assurer que les dommages potentiels seront minimisés et limités même si un attaquant obtient un accès.



Atténuer les risques de vulnérabilité liés à Microsoft

L'application de correctifs en temps opportun est un moyen important de minimiser le risque d'une violation liée à une vulnérabilité.

Pourtant, en utilisant seulement cette stratégie, les organisations continueront de courir le risque de subir des failles zero-day. De plus, la correction de vulnérabilités n'est pas toujours pratique ou souhaitable pour une organisation. C'est pourquoi il est essentiel de mettre en place des défenses de sécurité proactives, telles que le principe de moindre privilège.

Cinq stratégies d'atténuation indispensables pour sécuriser votre environnement Microsoft :

- 1 Mettre en œuvre une gestion des vulnérabilités :** Trouver, hiérarchiser et déterminer une méthode d'atténuation pour toutes les vulnérabilités. Gardez à l'esprit qu'en appliquant au plus tôt des correctifs, vous pouvez éviter qu'une vulnérabilité d'apparence innocente ait un effet boule de neige menant à une menace plus grande
- 2 Appliquer le principe du moindre privilège, par exemple en supprimant les droits admins locaux :** Cette approche proactive peut fournir une protection très efficace, même en l'absence de correctifs. La suppression des droits admins locaux et le contrôle de ce qui est exécuté ont historiquement atténué 75 % des vulnérabilités critiques de Microsoft, comme nous l'avons démontré dans les rapports antérieurs où les données sont disponibles. Cela signifie qu'en l'absence de droits admins, la vulnérabilité ne peut pas être exploitée, même si elle n'a pas été corrigée. Une approche de moindre privilège, qui est également un élément central des modèles de sécurité zero-trust, peut aider à briser plusieurs points de la chaîne d'attaque : du piratage de compte au mouvement latéral, en passant par l'élévation des privilèges, etc.
- 3 Suivre les protocoles de renforcement de la sécurité :** Assurez-vous en permanence que votre système d'exploitation et vos logiciels tiers sont à jour et qu'il n'y ait pas de logiciel en fin de vie dans votre environnement. En outre, supprimez les privilèges, les accès et les comptes inutiles pour réduire davantage la surface d'attaque.
- 4 Sécurisez les chemins d'accès distants :** Le protocole RDP (Remote Desktop Protocol) de Microsoft, les VPN et de nombreuses autres technologies d'accès à distance courantes, servent de plus en plus à des fins dépassant leurs cas d'usage appropriés, ce qui entraîne des risques et des failles de sécurité. Le ransomware en particulier utilise souvent le RDP comme point d'entrée. Vérifiez que le RDP ne soit pas exposé à Internet. Ne permettez pas que des VPN et des dispositifs BYOD puissent interagir. Remplacez vos VPN, ou ajoutez-y des contrôles de sécurité zero-trust pour l'accès des fournisseurs et les accès privilégiés.
- 5 Faites preuve de vigilance en ce qui concerne les menaces émergentes :** Comprendre les menaces contribue grandement à prendre des décisions plus avisées et à assurer votre sécurité. La dernière décennie a connu des changements considérables dans le paysage des menaces Microsoft. Avec le développement et le déploiement rapides des technologies à base d'IA, nous verrons probablement de nombreuses transformations à fort impact dans les menaces au cours de la prochaine décennie et au-delà.



Privileged Access Management (PAM) de BeyondTrust offre une ample variété d'avantages pour réduire le risque associé aux vulnérabilités critiques de Microsoft.

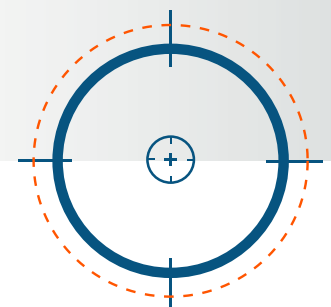
BeyondTrust protège les identités privilégiées, dimensionne les privilèges de façon pertinente et sécurise et audite les accès privilégiés dans toute l'entreprise.

Les utilisateurs s'appuient sur Privileged Access Management de BeyondTrust pour :

- Supprimer les droits admins et mettre en place une véritable application du moindre privilège, conforme aux principes zero-trust.
- Sécuriser les chemins d'accès à distance et l'infrastructure en veillant à ce que tous les accès des employés, des fournisseurs et d'autres personnes soient contrôlés et vérifiés de manière granulaire.
- Empêcher le détournement de compte et l'élévation des privilèges en gérant en toute sécurité tous les identifiants ainsi que les secrets humains et machine privilégiés qui touchent l'entreprise.
- Gérer, surveiller et auditer chaque session privilégiée.
- Obtenir une visibilité supérieure quant aux chemins d'accès potentiels de sorte que les accès puissent être proactivement dimensionnés et que les vecteurs d'attaque soient éliminés.
- Répondre aux exigences rigoureuses en matière de conformité en fournissant des rapports faciles d'accès sur toutes les activités privilégiées et d'autres informations.
- Être admissible à une cyberassurance en se dotant d'un certain nombre de contrôles de sécurité demandés par les assureurs et leurs courtiers.

Avec BeyondTrust, les organisations profitent d'une protection proactive contre les menaces externes (ransomware, malware, etc.) et les menaces internes.

En savoir plus.





Qu'avons-nous appris après une décennie d'analyse des vulnérabilités Microsoft ?

Conclusion

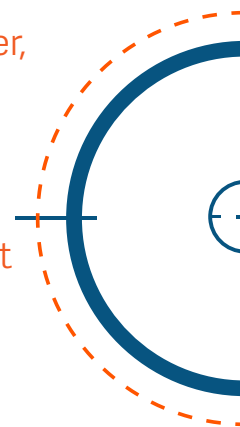
En 2022, le nombre total de vulnérabilités Microsoft a atteint un niveau record qui a presque quadruplé depuis l'édition initiale de ce rapport il y a dix ans. Les vulnérabilités Microsoft liées à l'élévation de privilèges ont grimpé en flèche de 650 % au cours des dix dernières années. Durant cette période, les nouveaux produits Microsoft ont entraîné l'augmentation globale du total des vulnérabilités, celles liées à Azure et Dynamics 365 ayant augmenté de 159 % au cours de la seule année écoulée.

Alors que le nombre total de vulnérabilités de Microsoft continue d'augmenter - ce qui est symptomatique d'une entreprise en pleine croissance et d'une surface d'attaque en expansion - les initiatives de réduction des menaces de Microsoft et son engagement à adopter des correctifs et des protocoles de sécurité ont conduit à une diminution constante des vulnérabilités critiques sur cinq ans. En 2022, 6,9 % des vulnérabilités de Microsoft seulement étaient classées comme « critiques », contre 44 % en 2013.

Il y a dix ans environ (2014), Microsoft a adopté une stratégie « mobile-first, cloud-first ». À l'époque, cette stratégie représentait un revirement, mais désormais, elle constitue une base de l'approche de Microsoft, et de celle de plus en plus d'entreprises dans le monde entier. Au cours de la décennie à venir, des technologies autrefois considérées comme ayant un intérêt hypothétique, par exemple l'IA, seront activement mises au point, produites et intégrées chez Microsoft. Bien que ces technologies soient très prometteuses, pour les organisations ou l'humanité, elles représentent de nouvelles surfaces d'attaque et des vecteurs de menace potentiels. Des vulnérabilités sont susceptibles d'émerger d'une manière jamais vue auparavant.

Nous avons appris que, tout comme la mort et les impôts, les vulnérabilités (du moins lorsque des logiciels sont concernés) sont inévitables.

Alors que le paysage technologique entame sa prochaine phase d'évolution, le nombre de vulnérabilités devrait continuer à augmenter, de nouvelles menaces continueront à émerger du cyberspace, et nous continuerons à vous faire part de nos réflexions et de nos tactiques de défense.





S'il existe une lueur d'espoir au regard des dix dernières années de vulnérabilités, c'est le fait que les moyens fondamentaux d'atténuer ces risques sont restés constants pendant plus d'une décennie.

Les concepts de moindre privilège décrits par le [ministère américain de la Défense en 1985](#) sont intemporels. L'application du principe de moindre privilège s'est révélée être tout aussi pertinente pour les systèmes cloud et les dispositifs IoT actuels qu'elle l'était pour les systèmes d'antan (dont certains sont toujours opérationnels).

Les organisations qui réussissent à mettre en place des contrôles de sécurité préventifs et proactifs continueront d'être bien mieux préparées pour résister aux menaces de demain, comme ce fut le cas au cours de la dernière décennie. Si vous ne deviez retenir qu'un seul conseil à la lecture de ce rapport pour protéger votre organisation contre les menaces incessantes, ce serait de continuer à mettre en œuvre et à appliquer les contrôles de sécurité fondamentaux dont l'efficacité a été prouvée encore et encore face aux plus grandes menaces de la décennie.

Méthodologie

Chaque mardi, Microsoft publie son « Patch Tuesday » et des bulletins de sécurité dévoilant des correctifs pour toutes les vulnérabilités affectant les produits Microsoft. Le Microsoft Vulnerabilities Report de BeyondTrust, publié annuellement, compile ces publications en une présentation couvrant toute l'année et analyse leurs données, pour créer une vue générale des tendances liées aux vulnérabilités.

Jusqu'à novembre 2020, Microsoft utilisait sa propre méthode de partage des détails des CVE via son Security Update Guide.

Le format de reporting antérieur comportait un résumé analytique pour chaque vulnérabilité signalée qui incluait les aspects suivants :

- Les clients/utilisateurs dont les comptes sont configurés pour avoir moins de droits utilisateur sur le système pourraient être moins impactés que ceux qui fonctionnent avec des droits admins.
- Si l'utilisateur actuel est connecté au moyen de droits admins, un attaquant pourrait prendre le contrôle de la machine affectée.

À partir de ce résumé, les chercheurs en sécurité ont pu déduire si une vulnérabilité donnée (en particulier les vulnérabilités critiques) aurait pu être atténuée si les droits admins avaient été retirés à l'utilisateur.

En 2021 cependant, Microsoft a changé de méthodologie et a adopté le CVSS (Common Vulnerability Scoring System). En 2022, Microsoft a continué d'utiliser le système CVSS 3.1 pour noter les vulnérabilités, mais a commencé à classer les gravités en fonction de son propre Security Update Severity Rating System.

La méthodologie CVSS permet aux vulnérabilités Microsoft d'être recoupées plus facilement avec des bugs tiers, ce qui simplifie

certaines analyses. Le Security Update Severity Rating System de Microsoft permet à chaque vulnérabilité d'être évaluée en fonction du pire résultat théorique en cas d'exploitation.

Toutefois, une conséquence malheureuse de ce changement a été la perte de la capacité à déterminer l'impact des droits admins sur les vulnérabilités critiques.

Non seulement les risques liés aux accès surprivilegiés demeurent fortement intacts, mais les vecteurs d'attaque privilégiée augmentent aussi rapidement avec l'expansion du cloud.

Ainsi, bien que les statistiques sur les droits admins soient absentes du rapport cette année, il est impératif que les organisations ne fassent pas preuve de complaisance. La suppression des droits admins reste un élément clé dans l'application du principe de moindre privilège, ainsi que de l'activation de l'approche zero-trust.

Précision des données sur les vulnérabilités

Un certain nombre de généralisations ont été faites pour chaque vulnérabilité, comme suit :

- Chaque vulnérabilité a été classée en fonction du degré de gravité le plus élevé de tous les cas où elle est apparue plusieurs fois.
- Chaque vulnérabilité a été classée selon le type le plus répandu pour toutes les occurrences de cette vulnérabilité.
- Les versions de produit n'ont pas été prises en compte.
- Les combinaisons de produits n'ont pas été prises en compte.
- Les vulnérabilités ont été comptabilisées à la fois pour le logiciel et la version, le cas échéant (par exemple, une vulnérabilité pour Microsoft Edge sur Windows 10 est considérée comme une vulnérabilité à la fois pour Microsoft Edge et Windows).



> Ressources supplémentaires

OUTIL GRATUIT [Privileged Access Discovery Application](#)

Utilisez l'outil gratuit le plus puissant disponible pour analyser votre environnement et mettre en évidence les comptes surprivilégiés, les comptes de services, les comptes inutilisés, les identifiants privilégiés, les outils d'accès distant et plus encore.

PASSER LE TEST Besoin d'une alternative aux VPN ? Passez le test de Remote Access

Découvrez si votre équipe dispose des outils appropriés pour les accès distants sécurisés afin de gérer de grandes quantités d'utilisateurs qui se connectent à distance à votre réseau.

LIVRE BLANC [Cybersecurity Survival Guide](#)

Obtenez des astuces et des stratégies pour vous aider à éviter les pièges dans le paysage de la cybersécurité.

CHECKLIST [Cybersecurity Insurance Checklist](#)

Accédez aux conseils et aux stratégies qui vous aideront à éviter les pièges du paysage de la cybersécurité.



BeyondTrust est le leader mondial de la sécurité intelligente de l'identité et de l'accès, permettant aux organisations de protéger les identités, de contrer les menaces et de fournir un accès dynamique afin de renforcer et de sécuriser l'environnement de travail hybride. Nos produits intégrés et notre plate-forme offrent la solution de gestion des accès privilégiés (PAM) la plus avancée du secteur, permettant aux organisations de réduire rapidement leur surface d'attaque dans les environnements traditionnels, cloud et hybrides.

BeyondTrust protège toutes les identités privilégiées, les accès et les endpoints dans un environnement informatique contre les menaces de sécurité, tout en créant une expérience utilisateur supérieure et des efficacités opérationnelles. Avec un héritage d'innovation et un engagement indéfectible envers les clients, les solutions BeyondTrust sont faciles à déployer, à gérer et à faire évoluer à mesure que les entreprises évoluent. 20 000 utilisateurs nous font confiance, dont 75 entreprises du classement Fortune 100, ainsi qu'un réseau mondial de partenaires. Pour en savoir plus, rendez-vous sur www.beyondtrust.com.

beyondtrust.com/fr