BeyondTrust

Les organisations traversent-elles une crise d'identité ?

2024 Rapport sur les Vulnérabilités Microsoft

Bénéficiez d'informations fondées sur des recherches et d'analyses d'experts du secteur pour mieux protéger votre environnement Microsoft en 2024 et au-delà.

BeyondTrust

TABLE DES MATIÈRES

Résumé

Après l'édition de l'an passé pour 10e anniversaire du rapport, nous passons cette année à la vitesse supérieure en posant une question clé sur le paysage des vulnérabilités de Microsoft :

« Les organisations traversent-elles une crise d'identité ? »

Au cours de ses 11 années de publication, le rapport sur les vulnérabilités de Microsoft a été téléchargé plus de 16 000 fois et a aidé des milliers d'utilisateurs grâce à son analyse détaillée des données et de ses conclusions d'experts pour améliorer leur cyberdéfense.

L'édition de cette année ne se contente pas seulement de disséquer les données de 2023 sur les vulnérabilités de Microsoft, mais évalue également la manière dont ces vulnérabilités sont exploitées dans le cadre d'attaques basées sur l'identité. Le rapport met également en lumière certains des CVE les plus importants de 2023 (scores de gravité CVSS 9.0+), explique comment ils sont exploités par les attaquants et comment ils peuvent être atténués.

Un groupe d'experts en cybersécurité parmi les plus réputés au monde se prononcera sur les conclusions du rapport, nous examinerons ensemble les menaces émergentes, les nouvelles vulnérabilités et les moyens de renforcer la cyber-résilience au sein de l'entreprise.

Lisez la suite pour mieux comprendre, identifier et traiter les risques auxquels votre organisation est confrontée au sein de l'écosystème Microsoft.

Principales conclusions et faits marquants

Principaux résultats

Après avoir atteint un nombre record de vulnérabilités Microsoft signalées en 2022, le nombre total de vulnérabilités a légèrement diminué en 2023.

Si l'on considère la tendance générale, le nombre de vulnérabilités de Microsoft a atteint un palier depuis 2020.

Le nombre total de vulnérabilités reste stable depuis 4 ans, proche de son plus haut niveau jamais enregistré.
Bien qu'ils aient légèrement diminué (de 5%), passant de 1 292 à 1 228 en 2023, le nombre de vulnérabilités totales reste très élevé, se maintenant entre 1 200 et 1 300 au cours des quatre dernières années (depuis 2020).

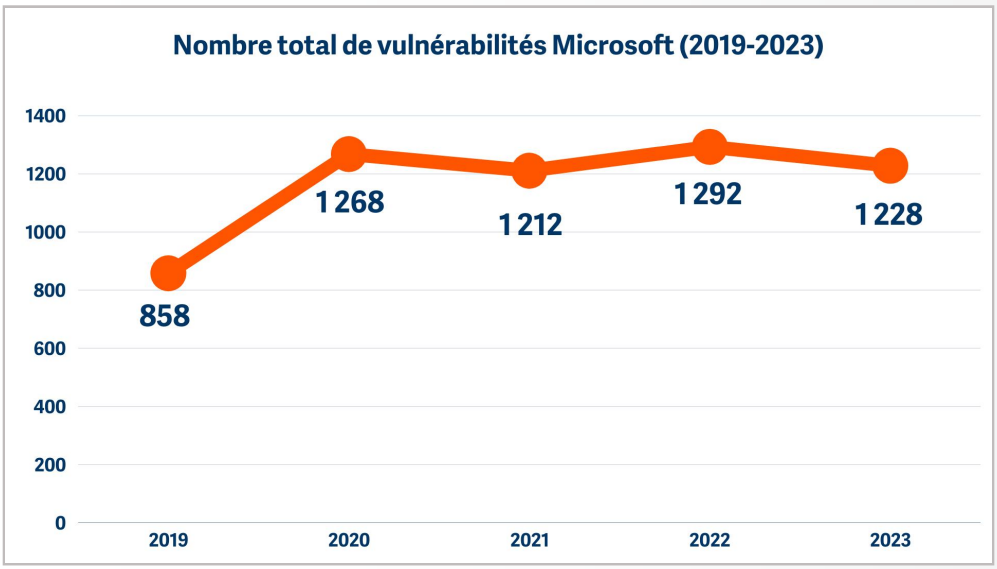
La catégorie de vulnérabilité "Elévation de privilèges" continue de dominer. Poursuivant la tendance des années post-pandémiques, l'élévation des privilèges représentait 40 % (490) du total des vulnérabilités en 2023.

Le nombre total des vulnérabilités critiques poursuit sa tendance à la baisse. Les vulnérabilités critiques ont diminué de 6 % (84) en 2023 (5 de moins qu'en 2022).

Faits marquants

- Après la montée en flèche des vulnérabilités de Microsoft Azure et Dynamics 365 en 2022, elles ont presque diminué de moitié en 2023, passant de 114 à 63.
- Microsoft Edge a connu 249 vulnérabilités en 2023, dont une seule était critique.
- Il y avait 522 vulnérabilités Windows en 2023, dont 55 critiques.
- Microsoft Office a rencontré 62 vulnérabilités en 2023.
- Windows Server comptait 558 vulnérabilités en 2023, dont 57 critiques.
- Les vulnérabilités par déni de service ont grimpé de 51 % pour atteindre un niveau record de 109 en 2023. L'usurpation d'identité a eu une augmentation spectaculaire de 190 %, passant de 31 à 90 vulnérabilités.

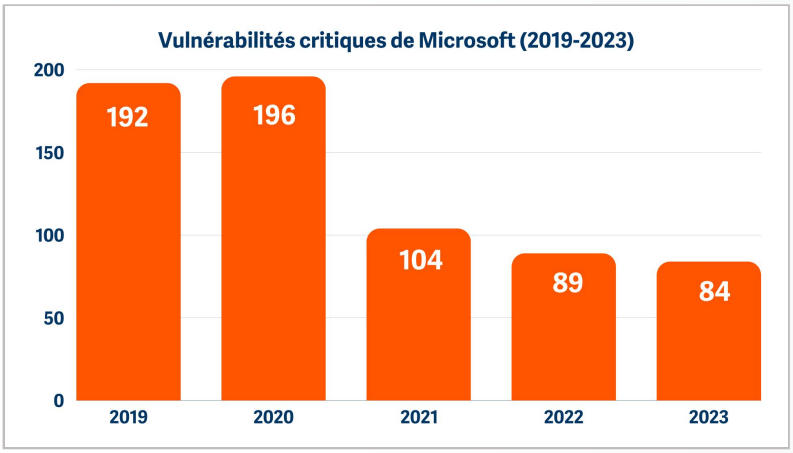
Tendance sur 5 ans



Le nombre total de vulnérabilités s'est stabilisé, se maintenant entre 1 200 et 1 300 au cours des quatre dernières années.

Suite à l'augmentation spectaculaire des vulnérabilités Microsoft en 2020, nous avons observé que le nombre total de vulnérabilités plafonnait au cours des quatre dernières années, la plage de fluctuations restant dans une fenêtre de 7%.

Le nombre total de vulnérabilités a atteint 1 228 en 2023, ce qui représente une diminution de 5 % par rapport à l'année précédente, après avoir atteint un niveau record de 1 292 en 2022.

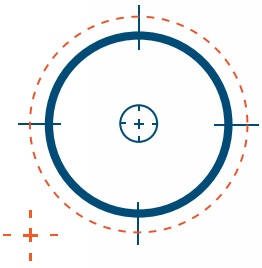


Les vulnérabilités critiques ont poursuivi leur tendance à la baisse en 2023, le rythme a ralenti.

De même, les vulnérabilités critiques sont restées stables, passant légèrement de 89 en 2022 à 84 en 2023. En termes de vulnérabilités totales et critiques, cela fait des deux dernières années les plus cohérentes que nous ayons vues depuis les débuts de ce rapport il y a onze ans, sans changements majeurs dans les données de base.

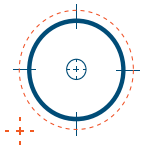
Si l'on examine la répartition des vulnérabilités critiques d'une année sur l'autre, on observe une tendance constante à la baisse. Les catégories Windows Desktop et Server sont toutes deux restées la principale source de vulnérabilités critiques jusqu'en 2023. Étant donné qu'elles partagent une base de code similaire, qui représente une évolution progressive du noyau Windows NT, ce n'est pas une surprise.

Comme nous l'avons indiqué dans le rapport de l'année dernière, certaines parties des systèmes d'exploitation Windows contiennent du code vieux de 20 ans, souvent oublié depuis longtemps, qui peut revenir nous nuir, même dans les versions les plus récentes de Windows. Au fil du temps, ces risques n'ont cessé de diminuer au fur et à mesure que les services et les fonctionnalités étaient actualisés. Cela explique en partie pourquoi nous constatons aujourd'hui une stabilité des données, que nous aborderons plus en détail ci-dessous.



Source majeure de risque pour toutes les organisations, les vulnérabilités critiques, lorsqu'elles sont exploitées, peuvent entraîner des événements de sécurité à fort impact. Ce sont ces vulnérabilités qui empêchent les administrateurs IT de dormir.

Que nous apprennent les données sur les vulnérabilités stables ?



La stabilité des données relatives aux vulnérabilités est un indicateur fort que les efforts globaux de sécurité à long terme portent leurs fruits.

Comme nous l'avons indiqué dans les rapports précédents, l'absence de fortes augmentations, ainsi que des chiffres en baisse constante, sont de bons indicateurs du fait que de nombreux efforts de sécurité à long terme de Microsoft portent leurs fruits.

Les produits existants, dont beaucoup ont été développés avant que Microsoft n'introduise son Security Development Lifecycle en 2004, sont arrivés en fin de vie (EOL), et des systèmes d'exploitation et des produits plus récents et plus sécurisés ont pris leur place. Les technologies cloud sont arrivées à maturité et les investissements en matière de sécurité ont porté leurs fruits.

Si l'on remonte seulement trois ans en arrière, le tableau est radicalement différent. En 2020, le nombre de vulnérabilités critiques était supérieur de 133 % à ce qu'il était en 2023. Bien que les données de cette année n'aient pas révélé une diminution aussi importante des vulnérabilités critiques que celles des années précédentes, la tendance à la baisse se poursuit. Il s'agit d'une constatation rassurante, en particulier pour les équipes IT qui vivent et respirent la sécurité de leurs systèmes Microsoft.

Comprendre les vulnérabilités critiques de Microsoft

Le nombre total de vulnérabilités est un indicateur important de la santé d'un environnement, mais les vulnérabilités ne sont pas égales.

Certaines vulnérabilités peuvent présenter un risque essentiellement théorique (faible probabilité et faible impact) si elles sont exploitées. À l'opposé, d'autres vulnérabilités ont une forte probabilité d'être exploitées pouvant avoir un impact très négatif sur l'organisation.

La mesure du niveau d'impact d'une vulnérabilité est liée à son incidence 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 principes de base de la sécurité de l'information.

Les vulnérabilités classées comme "critiques" sont celles dont les caractéristiques font de leur exploitation un événement de sécurité à fort impact potentiel. La façon dont Microsoft classe la gravité d'une vulnérabilité est distincte de la probabilité d'exploitation.

Cependant, la probabilité d'exploitation est beaucoup plus dynamique, car les attaquants sont plus susceptibles d'exploiter une vulnérabilité connue.

L'exploitation de vulnérabilités « critiques » :

Risque de compromettre totalement un appareil ou une infrastructure.

A moins de conditions préalables. En général, l'attaque ne nécessite pas d'accès spécial, de privilèges ou de connaissances avancées.

Permet l'exécution du code sans interaction de l'utilisateur. Ils ne reposent généralement pas sur l'ingénierie sociale.

Ce sont ces types de vulnérabilités qui empêchent les administrateurs IT de dormir et qui constituent une source majeure de risques à laquelle les organisations doivent faire face partout dans le monde.

Comment Microsoft classe-t-il les vulnérabilités critiques ?

La base de données nationale sur les vulnérabilités (NVD) classe les vulnérabilités critiques comme celles ayant reçu un Système commun de notation des vulnérabilités (. CVSS) score de 9.0-10.0. Les lecteurs les plus enthousiastes des communiqués de Microsoft sur les vulnérabilités ont peut-être remarqué que, bien que Microsoft utilise désormais la notation CVSS 3.1 pour ses vulnérabilités, elle classe les degrés de gravité sur la base de son propre système d'évaluation de la gravité des mises à jour de sécurité. Ce système classe chaque vulnérabilité en fonction du pire résultat théorique en cas d'exploitation de cette vulnérabilité.

Cela signifie que :

Même si 33 vulnérabilités de Microsoft en 2023 ont obtenu une note de 9,0 ou plus (soit une augmentation de 50 % par rapport à 22 en 2022), ce qui les rend "critiques" selon le système de notation de National Vulnerability Database, Microsoft a classé 84 de ses vulnérabilités comme critiques en 2023 (soit une baisse de 6 % par rapport à 89 en 2022).

Notations CVSS 3.1

Gravité	Plage de scores de base
Aucune	0.0
Faible	0.1 - 3.9
Moyen	4.0 - 6.9
Élevé	7.0 - 8.9
Critique	9.0 -. 10.0

figue. 1 : Le système de notation National Vulnerability Database (NVD) pour classer les vulnérabilités critiques

Système d'évaluation des mises à jour de sécurité Microsoft | Note et description

Critique
Une vulnérabilité dont l'exploitation pourrait permettre l'exécution de code sans interaction de l'utilisateur. Ces scénarios incluent des logiciels malveillants à propagation automatique (par exemple . g. vers de réseau), ou des scénarios d'utilisation courante et évitables dans lesquels l'exécution de code se produit sans avertissements ni notifications. Cela peut signifier accéder à une page Web ou ouvrir un courrier électronique. Microsoft recommande aux clients d'appliquer immédiatement les mises à jour critiques.

Important
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.

Modéré
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.

Fig 2 : Le système d'évaluation de la gravité des mises à jour de sécurité de Microsoft, qui permet d'identifier les risques associés sur la base du pire résultat théorique en cas d'exploitation de la vulnérabilité.

La différence entre le score CVSS et le système d'évaluation de la gravité de Microsoft mérite d'être soulignée, non seulement lorsque l'on examine les données de ce rapport, mais également lorsque l'on étudie les risques dans votre organisation.

Les scores CVSS mesurent la gravité technique d'une vulnérabilité (c'est-à-dire si une vulnérabilité entraîne une perte de confidentialité partielle ou totale des données). Les scores CVSS ne mesurent pas le risque de cette vulnérabilité. Cela signifie que les scores CVSS seuls ne peuvent pas vous dire si une vulnérabilité aura un impact critique sur un système, ou si la perte limitée de certaines données hautement sensibles aurait un impact plus grave que la perte totale de données non sensibles.

Le système d'évaluation de la gravité de Microsoft est potentiellement bien plus utile qu'un score CVSS de base ou temporel pour les professionnels de la sécurité qui tentent de donner la priorité à la réduction des risques. Toutefois, il est important de connaître son propre environnement et ses propres risques afin de savoir comment prioriser les correctifs et/ou utiliser d'autres contrôles de renforcement de la sécurité et d'autres mesures d'atténuation.

Toutes les données fournies par le système d'évaluation de la gravité de Microsoft sont basées sur les informations disponibles à ce moment-là. Elles ne tiennent pas compte du contexte des modèles de menace 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.

En plus de leur Système d'évaluation de la gravité des mises à jour de sécurité, Microsoft a également publié un Indice d'exploitabilité pour aider les clients à comprendre la probabilité d'exploitation. Cela peut être une information utile pour ceux qui ont besoin d'aide pour prioriser les mises à jour de sécurité. Par mesure d'avertissement, ces informations reflètent la probabilité d'exploitation au moment où la mise à jour de sécurité a été publiée. Cela ne reflète peut-être pas l'exploitabilité réelle qui se développera dans les semaines ou les mois suivants. Il est préférable d'utiliser l'index pour établir des priorités à très court terme pour les mises à jour, plutôt que pour justifier un retard important dans l'application des correctifs.

Indice d'exploitabilité Microsoft

figue. 3 : L'Indice d'exploitabilité de Microsoft pour évaluer la probabilité d'exploitation au moment de la publication de la mise à jour de sécurité

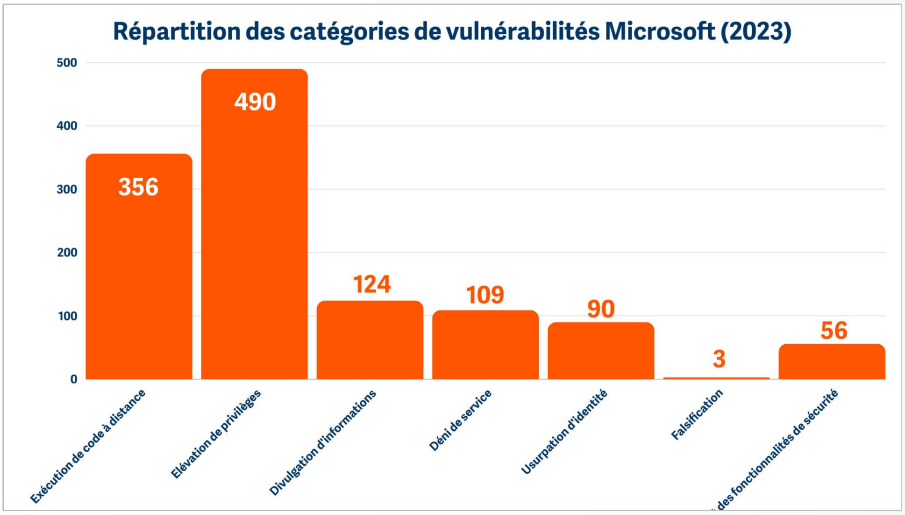
Index	Courte définition	Définition élargie
0	**Exploitation Détectée**	Microsoft a connaissance d'un cas d'exploitation de cette vulnérabilité. Par conséquent, les clients qui ont étudié la mise à jour de sécurité et déterminé son applicabilité dans leur environnement doivent traiter cette question avec la plus haute priorité.
1	**Exploitation Probable**	L'analyse de Microsoft a montré qu'un code d'exploitation pouvait être créé de manière à ce qu'un attaquant puisse exploiter cette vulnérabilité de manière cohérente. En outre, Microsoft a connaissance de cas antérieurs d'exploitation de ce type de vulnérabilité. Cela en fait une cible attrayante pour les attaquants et, par conséquent, une probabilité accrue de création d'exploits. Par conséquent, les clients qui ont examiné la mise à jour de sécurité et déterminé son applicabilité dans leur environnement devraient accorder une priorité plus élevée à cette question.
2	**Exploitation Moins probable**	L'analyse de Microsoft a montré que si un code d'exploitation pouvait être créé, un attaquant aurait probablement des difficultés à créer le code, ce qui nécessiterait une expertise et/ou un timing sophistiqué, et/ou des résultats variables lorsqu'il cible le produit affecté. En outre, Microsoft n'a pas observé récemment de tendance à l'exploitation active de ce type de vulnérabilité dans la nature. Cela en fait une cible moins attrayante pour les attaquants. Cela dit, les clients qui ont examiné la mise à jour de sécurité et déterminé son applicabilité dans leur environnement doivent toujours la considérer comme une mise à jour importante. S'ils donnent la priorité à d'autres vulnérabilités hautement exploitables, ils pourraient la classer plus bas dans leur priorité de déploiement.
3	**Exploitation Peu probable**	L'analyse de Microsoft montre qu'il est peu probable qu'un code d'exploitation fonctionnant correctement soit utilisé dans le cadre d'attaques réelles. Cela signifie que même s'il est possible de publier un code d'exploitation susceptible de déclencher la vulnérabilité et de provoquer un comportement anormal, l'impact total de l'exploitation sera plus limité. En outre, Microsoft n'a pas observé de cas d'exploitation active de ce type de vulnérabilité dans le passé. Par conséquent, le risque réel d'exploitation de la vulnérabilité est nettement plus faible. Par conséquent, les clients qui ont examiné la mise à jour de sécurité pour déterminer son applicabilité dans leur environnement pourraient donner la priorité à cette mise à jour par rapport à d'autres vulnérabilités dans une version.

Analyse approfondie des données sur les vulnérabilités

Vulnérabilités par catégorie

Chaque bulletin de sécurité Microsoft comprend une ou plusieurs vulnérabilités, qui s'appliquent à un ou plusieurs produits Microsoft.

Microsoft classe généralement les vulnérabilités dans les catégories suivantes : Exécution de code à distance (RCE), élévation de privilèges (EoP), divulgation d'informations, déni de service (. DDoS), usurpation d'identité, falsification et contournement des fonctionnalités de sécurité.



L'élévation de privilèges reste la #1 catégorie de vulnérabilité, malgré une baisse significative de 31 %, passant de 715 à 490 par rapport à l'année précédente.

Catégories de vulnérabilités Microsoft (2013-2022)

	2019	2020	2021	2022	2023
Exécution de code à distance	323	345	326	314	356
Élévation de privilèges	198	559	588	715	490
Divulgation d'informations	177	179	129	114	124
Déni de service	52	46	55	72	109
Usurpation d'identité	63	104	66	31	90
Falsification	8	7	3	4	3
Contournement des fonctionnalités de sécurité	38	30	44	42	56

L'exécution de code à distance brise sa tendance à la baisse en 2023, augmentant de 13 % pour atteindre 356, le nombre le plus élevé que nous ayons vu depuis le début de ce rapport.

L'exécution de code à distance et l'élévation de privilèges restent les principales catégories de vulnérabilités, soulignant une fois de plus les objectifs familiers des acteurs malveillants.

L'élévation de privilèges reste la catégorie de vulnérabilité #1 en 2023.

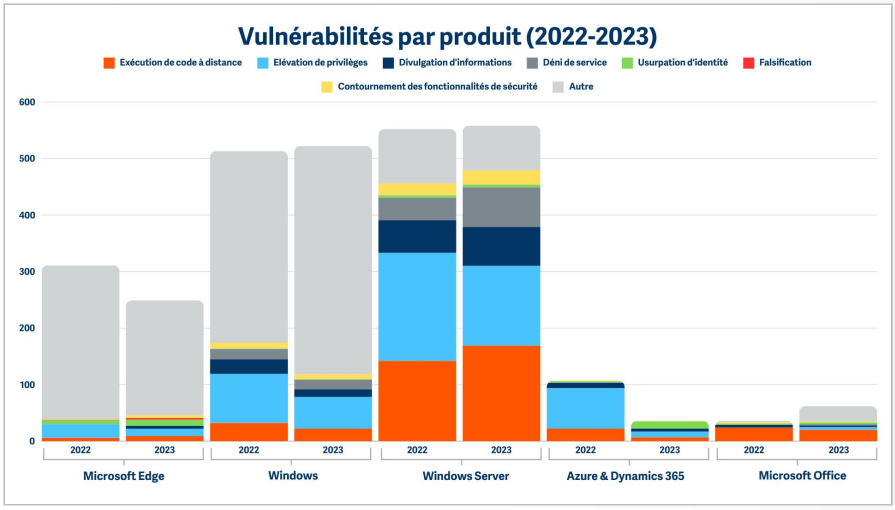
L'élévation des privilèges a poursuivi sa tendance post-2019 et reste la #1 catégorie de vulnérabilité en 2023, suivie par l'exécution de code à distance. Ce n'est pas surprenant car cela correspond directement aux tactiques de menace connues.

Les deux principales tactiques des acteurs de la menace sont les suivantes :

1. Faire exécuter leur code (https://attaque.mitre.org/tactics/TA0002/)
2. Accéder aux privilèges nécessaires pour poursuivre leurs objectifs (https://attaque.mitre.org/tactics/TA0004/)

La bonne nouvelle cette année est, même si les vulnérabilités sur l'élévation de privilèges restent la catégorie de vulnérabilités #1, elles ont diminué de 715 à 490, soit une baisse de 31%. Lorsque nous examinons les données, nous pouvons clairement voir que ces diminutions proviennent principalement de réductions des vulnérabilités Azure et Windows Server, comme le montre la figure ci-dessous.

C'est une bonne nouvelle, étant donné que ces systèmes sont souvent accessibles au public et beaucoup plus susceptibles de contenir de grandes quantités de données sensibles et des comptes de service privilégiés, par exemple : un système Windows Desktop.



Azure et Windows Server affichent tous deux une réduction significative des vulnérabilités EoP. Azure est passé de 72 vulnérabilités EoP en 2022 à 10 en 2023 (une diminution massive de 86%). Windows Server est passé de 191 à 141 (une diminution de 26%).

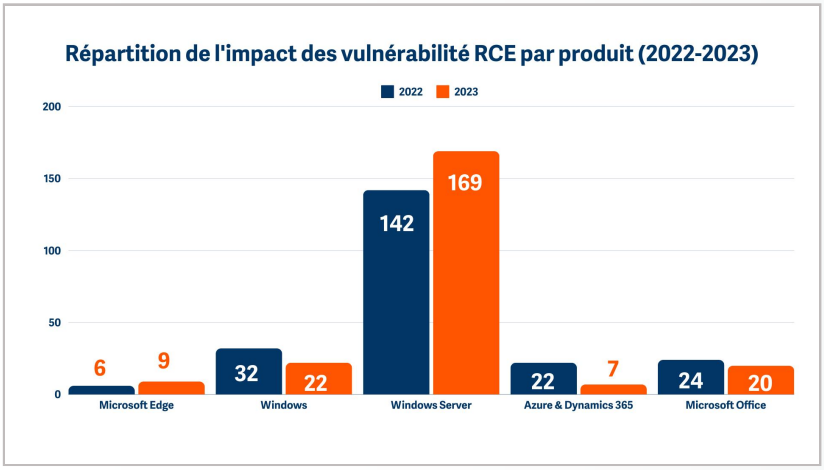
En général, la diminution des vulnérabilités de catégorie “élévation de privilèges” est une tendance très positive qui réduit directement les options d’un acteur malveillant lors du déploiement d’une menace nécessitant des privilèges élevés pour s’exécuter.

Cependant, vous ne pouvez pas vous fier uniquement à l'absence de vulnérabilités de catégorie “élévation de privilèges” pour protéger l'accès aux privilèges.

Il est toujours essentiel de maintenir une stratégie robuste de gestion des accès aux privilèges pour supprimer et sécuriser les privilèges au sein d'un environnement afin d'éviter qu'ils ne tombent entre les mains d'un attaquant.

L'exécution de code à distance vient juste après l'élévation des privilèges en 2023

Arrive en deuxième position la catégorie de vulnérabilités "exécution de code à distance (RCE)", qui est passée de 314 à 356 en 2023 (une augmentation de 13%). Alors que dans de nombreux domaines de produits, tels qu'Azure, Office et Windows (désormais principalement constitués de données Windows 10 et 11), nous avons constaté une diminution du RCE, cela a été compensé cette année par une augmentation du côté de Windows Server.



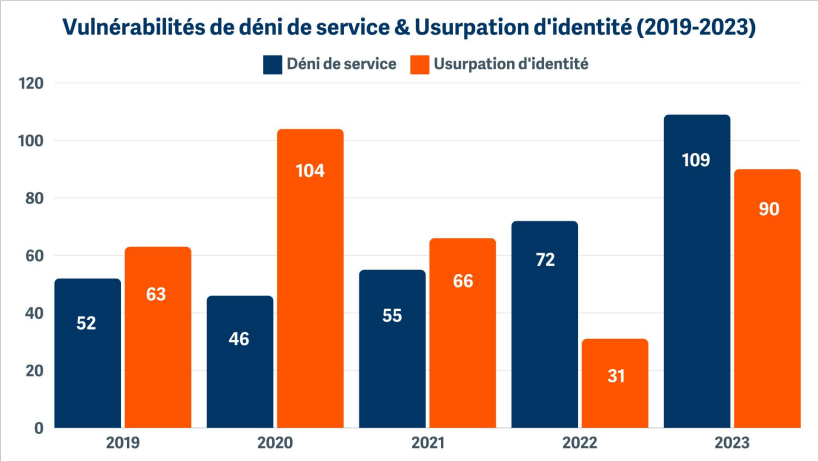
Les vulnérabilités RCE sur Windows Server sont passées de 142 à 169 en 2023, soit une augmentation de 19 %.

L'augmentation des vulnérabilités RCE de Windows Server n'est pas causée par un composant particulier mais est largement répartie sur différents services et fonctionnalités. En fait, bon nombre de ces détections résultent de la collaboration accrue de Microsoft avec sa communauté de recherche en sécurité. Il semble notamment que cette collaboration porte ses fruits car bon nombre de ces vulnérabilités ont été divulguées directement à Microsoft et corrigées avant d'être divulguées publiquement ou d'être exploitées.

Risque, ingénierie inverse et chercheurs : la course continue.

Les correctifs apportés en temps opportun permettent aux organisations de garder une longueur d'avance sur la majorité des acteurs de la menace, à condition que les organisations déploient les correctifs en temps voulu. Une fois qu'une vulnérabilité est divulguée et que les correctifs sont publiés, la course est lancée pour réussir à appliquer les correctifs avant qu'un acteur de la menace ne fasse de l'ingénierie inverse ou que la vulnérabilité ne soit rendue publique.
Les chercheurs et les acteurs de la menace ont réussi à inverser les correctifs pour trouver des solutions de contournement exploitables ou d'autres vulnérabilités dans des zones de code récemment corrigées. Comme le dit le proverbe, il n'y a pas de fumée sans feu, et comme nous l'avons souligné dans le rapport de l'année dernière, les vulnérabilités peuvent commencer à faire boule de neige lorsque l'attention est attirée sur un élément qui pourrait contenir plusieurs zones de code exploitables.

Les vulnérabilités de déni de service et d'usurpation d'identité augmentent considérablement en 2023



Les vulnérabilités de déni de service ont atteint un niveau record en 2023, grimpant de 51 %, passant de 72 en 2022 à 109 en 2023, tandis que l'usurpation d'identité a connu une augmentation spectaculaire de 190 %, passant de 31 en 2022 à 90 en 2023.

Lorsque nous réfléchissons à la sécurité des informations, nous nous concentrons souvent sur la garantie de la confidentialité et de l'intégrité des données, mais perturber la disponibilité des données peut également avoir un impact dévastateur. Les exploits par déni de service (DoS) peuvent être utilisés pour perturber la disponibilité des données et poser des problèmes aux opérations commerciales de la même manière que les ransomwares.

Que pouvons-nous apprendre sur les catégories de vulnérabilités de cette année ?

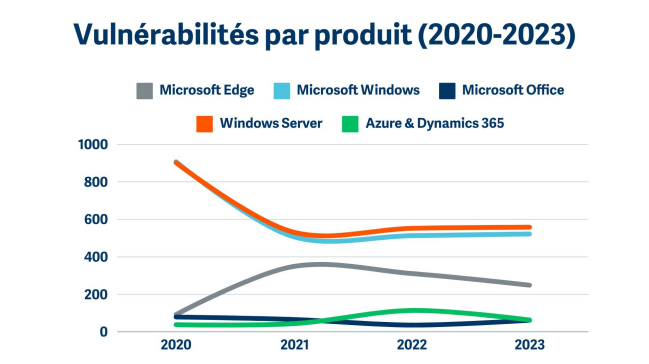
À mesure que les vulnérabilités globales se stabilisent, les acteurs de menace se concentrent davantage sur les identités.

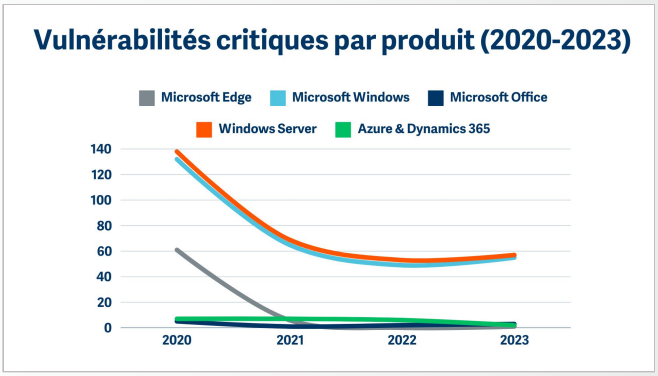
Lorsqu'il s'agit de faire exécuter du code, les auteurs de menaces n'ont pas d'autres choix que l'exploitation des vulnérabilités. Ils peuvent utiliser l'ingénierie sociale ou des identifiants volées pour introduire leur code dans un environnement sans avoir besoin d'une vulnérabilité logicielle. De même, lorsqu'il s'agit d'élever des privilèges, il peut être plus facile de pirater un compte déjà privilégié que d'exploiter une vulnérabilité logicielle ou une mauvaise configuration de l'environnement pour accéder aux privilèges requis.

À mesure que le nombre global de vulnérabilités Microsoft se stabilise et que le nombre de vulnérabilités critiques diminue, nous constatons que les attaquants concentreront beaucoup plus leur attention sur les identités.

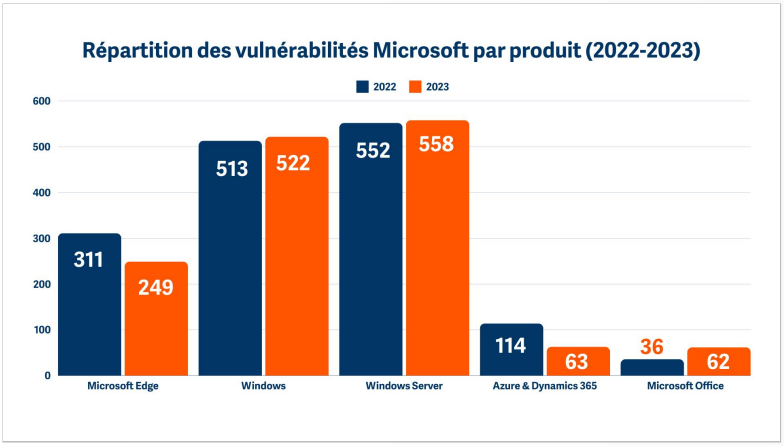
Cependant, cela ne signifie pas que nous pouvons faire preuve de complaisance face aux vulnérabilités logicielles. Non seulement il existe de nombreuses vulnérabilités, mais il existe également un certain nombre de systèmes non corrigés qui restent vulnérables aux exploits pour lesquels des correctifs étaient disponibles il y a des mois ou des années. Ces vulnérabilités connues permettent aux acteurs malveillants de lancer très facilement une attaque réussie.

Vulnérabilités par produit

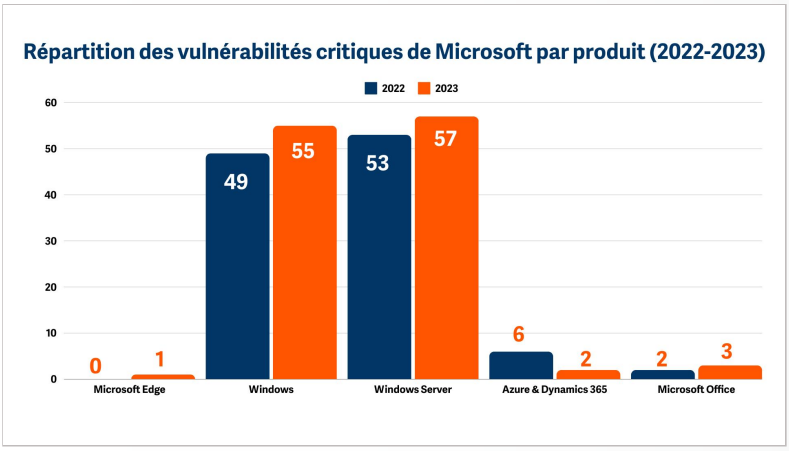




Dans l'ensemble, les chiffres de vulnérabilité se sont stabilisés. Le nombre total de vulnérabilités reste stable depuis quatre ans, et les vulnérabilités critiques continuent de diminuer, bien que la baisse ait ralenti.



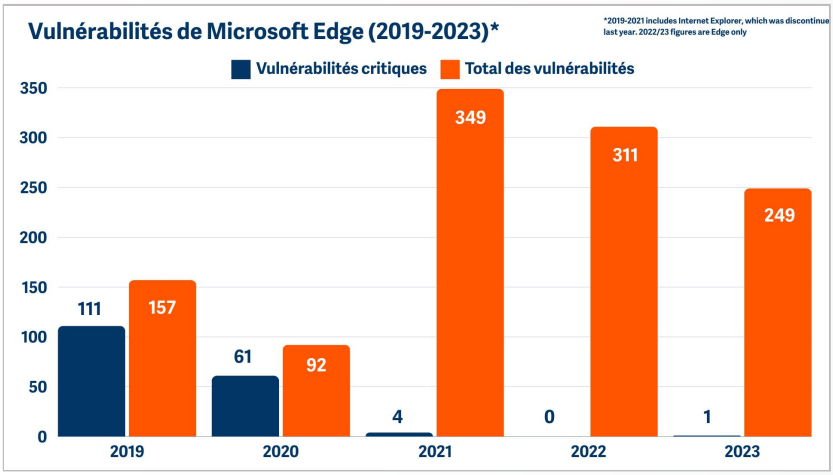
Les vulnérabilités de Windows Server ont légèrement augmenté en 2023. Le nombre total de vulnérabilités a légèrement augmenté, passant de 552 à 558 (1 %). Les vulnérabilités critiques ont également connu une légère augmentation, passant de 53 à 57.



La catégorie de vulnérabilité de Windows présente un schéma similaire, avec un nombre total de vulnérabilités augmentant de 513 à 522 (2 %) et des vulnérabilités critiques passant de 49 à 55.

Office et Edge continuent de montrer la voie et Azure corrige le cap après un pic de vulnérabilité record en 2022.

Microsoft Edge poursuit sa tendance à la baisse en matière de vulnérabilité



La base de code Chromium continue d'offrir des améliorations de sécurité significatives, marquées par une chute ces trois dernières années de vulnérabilités et d'exploits.

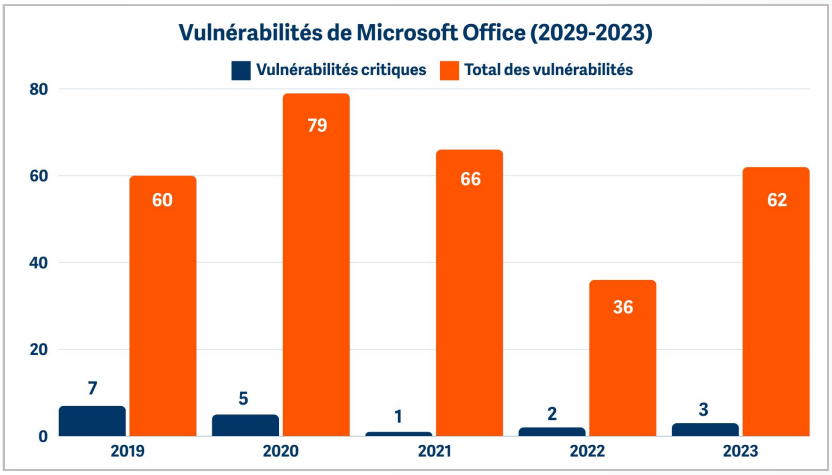
* 2019-2021 inclut Internet Explorer, qui a été abandonné l'année dernière. Les chiffres 2022/23 concernent uniquement Edge

Les navigateurs Web et les visualiseurs de documents ont toujours été un problème majeur en matière de vulnérabilités et de cyberattaques. Heureusement, Microsoft a fait des progrès significatifs en améliorant la sécurité de ces domaines.

Du côté du navigateur, le fait de déplacer Edge d'une base de code Microsoft personnalisée vers une base de code Chromium a apporté des améliorations significatives en matière de sécurité. L'abandon d'Internet Explorer a également contribué à faire en sorte que les exploits de téléchargement intempestif et les plugins Flash vulnérables appartiennent au passé.

Les vulnérabilités critiques dans Microsoft Edge ont chuté de 162 en 2017 à seulement 1 en 2023 (et 0 en 2022). Cela est dû en grande partie à l'adoption de la maturité de sécurité offerte par Chromium, qui sert de base à plusieurs navigateurs Web.

Les vulnérabilités de Microsoft Office atteignet à nouveau les niveaux de 2019-2021 en 2023



Les vulnérabilités d'Office augmentent au cours de 2022, mais poursuivent sa tendance globale à la baisse, obligeant les attaquants à adopter des méthodes d'attaque plus innovantes.

Du côté d'Office, nous avons constaté une tendance à la baisse similaire (bien que moins dramatique) pour les vulnérabilités totales et critiques, malgré une augmentation en 2023. Encore une fois, cela est en partie dû au fait que certaines des anciennes versions d'Office arrivent en fin de vie (EoL) et ne sont plus prises en charge.

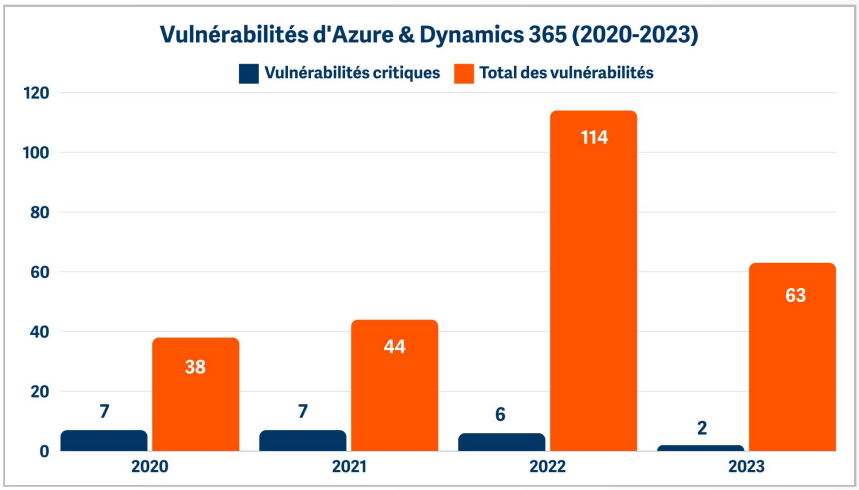
Les efforts déployés visant à empêcher le phishing et les logiciels malveillants via les applications Office continuent de forcer les attaquants à innover. Les contrôles introduits pour désactiver l'exécution automatique des macros dans les documents téléchargés ont bloqué certains chemins vers l'exécution de code à distance, obligeant les acteurs malveillants à rechercher des moyens plus créatifs pour exécuter du code à l'aide de documents et de fichiers malveillants.

L'un des nouveaux domaines les plus intéressants pour les vulnérabilités dans les applications Office est l'ajout par Microsoft de la prise en charge des fichiers SKP propriétaires de SketchUp Software en juin 2022. Ceci a été conçu pour faciliter l'importation de modèles 3D dans Word, Excel, PowerPoint et Outlook. Malheureusement, l'ajout de la prise en charge des fichiers 3D aux documents a également introduit une nouvelle dimension dans le paysage des vulnérabilités. L'équipe de ThreatLabz a découvert 117 vulnérabilités uniques qui ont été intégrées dans CVE-2023-33146, CVE-2023. -28285 et CVE-2023-29344.

Microsoft a ensuite créé un correctif pour corriger ces vulnérabilités, que l'équipe de ThreatLabz a réussi à contourner. Cela a conduit Microsoft à désactiver temporairement la prise en charge des fichiers SketchUp dans Microsoft 365 en juin 2023.

Bien que Microsoft prenne en charge les formats de fichiers 3D depuis un certain temps déjà, cet incident renforce la façon dont tout ajout de nouvelles fonctionnalités peuvent introduire des failles de sécurité. Dans ce cas, le code supplémentaire ajouté à la bibliothèque DLL MSOSPECTRE., responsable de l'analyse des formats de fichiers 3D, a exposé des vulnérabilités que Microsoft n'avait pas anticipées.

Les vulnérabilités d'Azure et Dynamics 365 ont été réduites de près de moitié en 2023.



Après avoir atteint un pic en 2022, les vulnérabilités d'Azure et Dynamics 365 ont connu une diminution impressionnante de 45 %, passant de 114 à 63 en 2023.

Après la montée en flèche des vulnérabilités de Microsoft Azure et Dynamics 365 en 2022, elles ont presque diminué de moitié en 2023, passant de 114 à 63. Compte tenu du grand nombre de produits et de services que couvre ce domaine, ces chiffres sont incroyablement bas.

Dans le rapport de l'année dernière, nous avons mis en évidence un outil de migration vers le cloud qui était à l'origine d'une proportion importante des vulnérabilités largement associées aux vulnérabilités de type SQLi (qui aurait cru qu'on parlerait encore de SQLi aujourd'hui !).

En 2023, cette tendance à la hausse s'est corrigée pour revenir au niveau attendu. Ce domaine de produits est principalement constitué de nouveaux codes conçus entièrement selon le cycle de vie de développement sécurisé de Microsoft, et nous pouvons clairement en voir les avantages par rapport aux anciens produits, qui présentent généralement des taux de vulnérabilités plus élevés.

> "Le renforcement proactif de la sécurité rompt souvent la chaîne d'exploitation de l'attaquant, en empêchant qu'un seul compte piraté ne permette à l'attaquant d'accéder à l'administration du domaine."
>
> **Jay Beale, PDG, CTO, InGuardians, Inc.**

Pleins feux sur les vulnérabilités

Comprendre les méthodes utilisées par les auteurs de menaces pour exploiter les vulnérabilités et infiltrer les organisations peut vous aider à prendre des décisions plus pertinentes pour protéger votre organisation.

Ralentissement du Print Spooler

La ruée vers les vulnérabilités (et les cibles principales des attaques par élévation de privilèges) touche peut-être à sa fin, mais cela ne signifie pas que les acteurs malveillants ne peuvent pas encore en profiter.

2018
« Le bug de l'imprimante » est identifié. Ce bug permet à un utilisateur non privilégié du réseau de déclencher à distance le service Print Spooler du contrôleur de domaine pour s'authentifier auprès d'un système arbitraire.
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 d'élévation de privilèges du Print Spooler de Windows sont divulguées. Initialement, ces vulnérabilités sont toutes des vecteurs d'attaque locaux, nécessitant que l'attaquant ait d'abord un accès direct au système exécutant le Print Spooler. Cependant, le résultat de chacun est qu'un attaquant pourrait exécuter du code arbitraire avec des privilèges système élevés.

CVE-2020-1030
CVE-2020-1048
CVE-2020-1070
CVE-2020-1337
CVE-2020-17001
CVE-2020-17014

Apparaît fin 2020. Contrairement aux attaques précédentes qui étaient exploitables localement, celle-ci est exploitable à distance, ce qui signifie que l'attaquant n'a besoin que d'être sur le réseau. Cet élément d'exploitation à distance rend cette vulnérabilité beaucoup plus grave. Toutefois, cette vulnérabilité n'a pas été divulguée publiquement et n'était pas connue pour être utilisée comme un exploit dans la nature.

L'effet boule de neige des vulnérabilités

Ce phénomène se produit lorsqu'une vulnérabilité est trouvée et corrigée, mais le processus attire un nouvel examen minutieux de la part de nouveaux chercheurs qui découvrent de nouvelles vulnérabilités, de nouveaux vecteurs d'attaque et de nouvelles façons de contourner les correctifs précédents, provoquant un effet boule de neige du nombre de vulnérabilités.

Le service Print Spooler, qui contient du code vieux de plus de 20 ans, est un bon exemple de l'effet boule de neige de vulnérabilité en action.

2021

16 vulnérabilités d'élévation de privilèges sur Print Spooler de Windows révélées. Print Spooler attire désormais l'attention de nombreux chercheurs comme un moyen intéressant de réaliser des attaques d'élévation de privilèges.

Le nombre de vulnérabilités EoP de Print Spooler de Windows révélées augmente rapidement à mesure que Microsoft joue à Whack-A-Mole avec des chercheurs qui ont trouvé des moyens de contourner les correctifs et continuent d'exploiter les vulnérabilités.

CVE-2021-. 34527 est la plus remarquable de la classe 2021 de vulnérabilités EoP du spouleur d'impression Windows.

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 d'exploitation, combinée au fait qu'il avait été divulgué publiquement et était activement utilisé, lui a valu le nom de "Print Nightmare."

Les 15 autres vulnérabilités de la classe 2021 sont les suivantes : 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 d'élévation de privilèges du Print Spooler de Windows sont révélées, soit plus du double de ce qui a été enregistré 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

2023

5 vulnérabilités d'élévation de privilèges du Print Spooler de Windows sont révélées, une réduction significative par rapport aux années précédentes.

CVE-2023-35325, CVE-2023-35302, CVE-2023-21765, CVE-2023-21760, CVE-2023-21678

Dans le rapport de l'année dernière, nous avons parlé de l'effet boule de neige autour des vulnérabilités de Print Spooler de Windows, dont le code vieux de plus de 20 ans avait été transmis à travers les versions de Windows, commençait à montrer son âge et à devenir la cible d'exploits. Le nombre de vulnérabilités du Print Spooler a presque doublé chaque année depuis la découverte en 2019 du « bug de l'imprimante » CVE-2019-0683, atteignant un pic en 2022 avec 35 vulnérabilités.

Cette ruée vers l'or semble être désormais limité à seulement cinq vulnérabilités en 2023 :CVE-2023-35325, CVE-2023-35302, CVE-2023-21765, CVE-2023-21760, CVE-2023-21678

Même s'il est encourageant de voir le volume se réduire, ces vulnérabilités ne sont pas insignifiantes et la majorité d'entre elles sont associées à une élévation de privilèges. Étant donné que le service de Print Spooler s'exécute en tant que SYSTEM (le niveau de privilège le plus élevé).

Contrairement aux années précédentes, il semble que Microsoft ait réussi à publier des correctifs avant qu'aucune de ces vulnérabilités ne soit divulguée publiquement ou exploitée dans la nature. Cela rassure sur le fait que des leçons ont été tirées dans ce domaine, mais démontre que ce n'est pas le moment de faire preuve de complaisance.

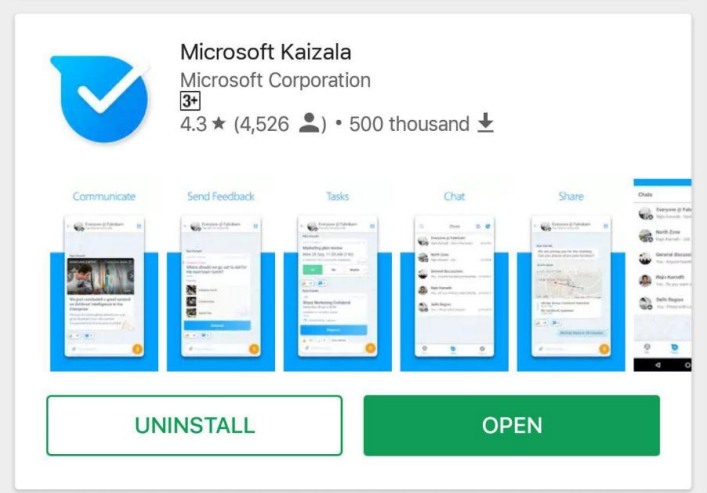
Il est temps de dire « au revoir »

Les logiciels en fin de vie ne sont plus pris en charge ni corrigés, ce qui représente un risque élevé pour les entreprises et une cible de choix pour les acteurs de menace.

De nombreux produits Microsoft ont connu une fin de vie en 2023. Cela signifie qu'ils ne recevront plus de correctifs de sécurité pour remédier aux vulnérabilités ou à d'autres problèmes.

Cette année, on notera la fin de vie des serveurs 2012 et 2012R2. En guise de cadeau d'adieu, ces deux systèmes d'exploitation pour serveurs ont reçu un ensemble de 65 correctifs, dont 11 sont critiques. Pour inciter les utilisateurs de ces systèmes d'exploitation à migrer vers Azure, Microsoft offre trois ans de mises à jour de sécurité étendues (ESU) au-delà de la date de fin de support (octobre 2023) sur Azure.

À l'autre extrémité du programme de mises à jour de sécurité étendues (ESU) de Microsoft se trouve Windows 7. Le système d'exploitation que vous pensiez déjà disparu depuis longtemps n'est plus couvert par le programme ESU de Microsoft. Comme cela signifie qu'il n'y a plus d'accès aux correctifs de sécurité critiques, il est certainement temps d'accélérer les plans de migration des systèmes Windows 7.



figue. 4 : Microsoft Kaizala est l'un des nombreux produits Microsoft qui sont arrivés en fin de vie (EOL) en 2023.

Il y a également eu quelques produits qui, comme le lecteur mp3 Zune de Microsoft, n'ont pas réussi à décoller et ont été retirés du marché sans qu'on y prête attention. En 2023, nous avons donc dit adieu à Microsoft Kaizala. Votre messagerie sécurisée optimisée pour le réseau 2G fait désormais partie de Teams et a été contrainte de se retirer.

Outlook n'a pas de chance avec CVE-2023. -23397

Une combinaison dangereuse de facilité d'exploitation et d'impact élevé a fait que cette vulnérabilité a attiré l'attention des administrateurs IT et des acteurs de la menace - en 2023.

Alors que nous continuons à nous réjouir du nombre historiquement bas de vulnérabilités critiques dans les produits Microsoft, il y a encore des vulnérabilités critiques qui font sourciller les professionnels de l'IT en 2023.

Contrairement à de nombreuses vulnérabilités antérieures, la vulnérabilité CVE-2023-23397 dans Microsoft Outlook ne nécessite aucune interaction de la part de l'utilisateur pour déclencher l'exploitation. Pire encore, la vulnérabilité touche toutes les versions de Microsoft Outlook pour Windows et permet à un attaquant d'obtenir des hachages d'identifiants Windows New Technology LAN Manager (NTLM) sensibles. Cette dangereuse combinaison de facilité d'exploitation et d'impact élevé s'est traduite par un score CVSS de base de 9,8, ce qui est plus que suffisant pour attirer l'attention des administrateurs informatiques et des acteurs de la menace.

La vulnérabilité est déclenchée lorsqu'un attaquant envoie une invitation ou un rendez-vous spécialement conçu l'adresse électronique d'une victime cible. Cette invitation contient des propriétés supplémentaires qui amènent Outlook à établir une connexion SMB et à déclencher l'authentification NTLM sur un serveur Internet contrôlé par l'attaquant. De là, l'attaquant peut capturer les hachages NTLM et les utiliser pour s'authentifier en tant que victime, ce qui conduit à une escalade potentielle des privilèges et à une compromission plus poussée de l'environnement.

Le véritable danger réside dans le fait que la vulnérabilité sous-jacente est déclenchée sans que l'utilisateur n'ait à ouvrir l'invitation. En fait, le déclencheur est le son de la notification de rappel.

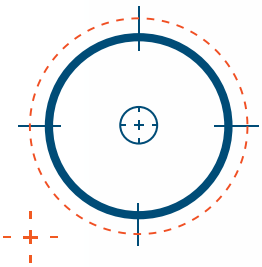
Bien qu'il s'agisse généralement d'un son prévisible pour vous rappeler qu'une réunion est sur le point d'avoir lieu, il existe une propriété « PidLidReminderFileParameter » qui peut être utilisée pour spécifier un fichier audio personnalisé à lire. Cette propriété peut être utilisée de manière abusive. Si un attaquant la définit comme une ressource distante sous son contrôle, Outlook se connectera et s'authentifiera, révélant finalement les hachages des identifiants de la victime.

Comme nous l'avons souligné dans le rapport de l'année dernière, des vulnérabilités importantes telles que celle-ci attirent souvent l'attention des auteurs de menaces et de la communauté des chercheurs, ce qui donne lieu à un jeu de Whack-A-Mole alors que Microsoft tente de publier des correctifs rapidement avant que les solutions de contournement ne soient découvertes. Le chercheur Dominic Chell a rapidement découvert que le correctif publié pour CVE-2023-23397 ne résolvait que le problème d'accès à distance, et que si un attaquant se trouvait au sein du réseau, il serait toujours capable d'exploiter cette vulnérabilité.

Bien que des mesures d'atténuation, telles que le blocage des connexions SMB sortantes ou l'ajout de membres au groupe d'utilisateurs protégés pour empêcher l'usage de l'authentification NTLM, soient disponibles, il s'agit d'une vulnérabilité critique à corriger en raison de la facilité avec laquelle elle peut être exploitée.

Comme cette vulnérabilité permet à un attaquant de capturer et potentiellement de rejouer les hachages NTLM pour s'authentifier en tant que victime cible, **il est important de toujours respecter le principe du moindre privilège. Moins la victime dispose de privilèges, moins le risque de compromission de compte et d'identité est élevé.**

Dans le pire des cas, un administrateur de domaine consulte des courriels à partir d'un compte hautement privilégié, ce qui permet à un pirate de prendre facilement le contrôle de l'ensemble du domaine. Dans un scénario idéal, vous auriez supprimé les privilèges d'administrateur local et sécurisé correctement les comptes à hauts privilèges, tels que les administrateurs de domaine, afin de garantir que, quelle que soit la vulnérabilité exploitée, les impacts seraient atténués.



Il est important de toujours respecter le principe du moindre privilège. Moins la victime dispose de privilèges, plus le risque de compromission de compte et d'identité est faible.

Le RomCom russe manque sa cible avec CVE-2023-36884

Ces campagnes de phishing élaborées ont ciblé des entités gouvernementales et de défense avec des pièces jointes malveillantes qui ont tiré parti d'un exploit d'exécution de code à distance de type "zero-day" pour contourner les protections de Mark of the Web. Il s'agit d'un exemple clair de la façon dont les attaquants ont innové pour contourner les protections alors que Microsoft continue d'améliorer la sécurité par défaut d'Office.

Au cours de l'été 2023, une campagne de phishing attribuée au groupe cybercriminel russe RomCom (également connu sous le nom de Storm-0978) a ciblé des entités gouvernementales et de défense en Europe et en Amérique du Nord en leur proposant des leurres liés au Congrès mondial ukrainien.

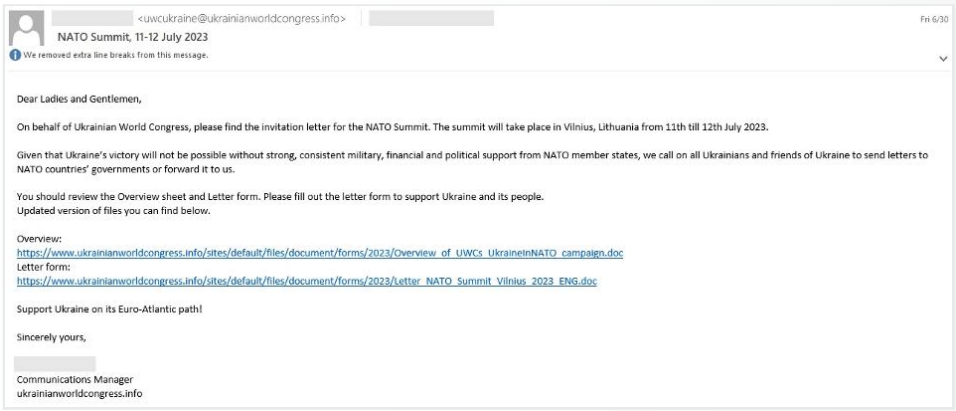


Figure 5 : une capture d'écran de la Campagne de phishing 2023 lancé par le groupe cybercriminel russe RomCom

L'objectif des leurres de phishing était de manipuler leurs cibles pour qu'elles téléchargent et ouvrent les documents malveillants via email.

Il convient de noter que les attaquants séparent souvent la source malveillante de l'e-mail de phishing en utilisant des liens dans l'e-mail ou dans un document joint. Cela rend les logiciels malveillants plus difficiles à détecter car le code malveillant est caché dans l'e-mail. Lorsque le courriel est analysé et que les solutions de sécurité tentent de scanner ces liens, ils peuvent être bloqués ou redirigés par le serveur qui héberge les sources.

RomCom est spécialisé dans ce type d'attaques par phising. Le groupe a déjà compromis un compte de messagerie du ministère ukrainien de la défense à la fin de l'année 2022. L'objectif de cette attaque était d'envoyer des emails de phising avec des pièces jointes au format PDF contenant des liens vers des sites web compromis hébergeant des logiciels malveillants voleurs d'informations.

Si l'utilisation de documents Office malveillants n'est pas nouvelle, cette campagne s'est distinguée par l'exploitation d'une vulnérabilité connue ultérieurement sous le nom de CVE-2023-36884.

Pour protéger les utilisateurs contre les documents malveillants, Microsoft attache une balise d'identification de zone, connue sous le nom de « Mark of the Web », aux fichiers téléchargés par les navigateurs et les emails. Cette balise contient un ID de zone qui indique si le fichier a été téléchargé depuis Internet ou un réseau local, ainsi que les URL d'où il provient.

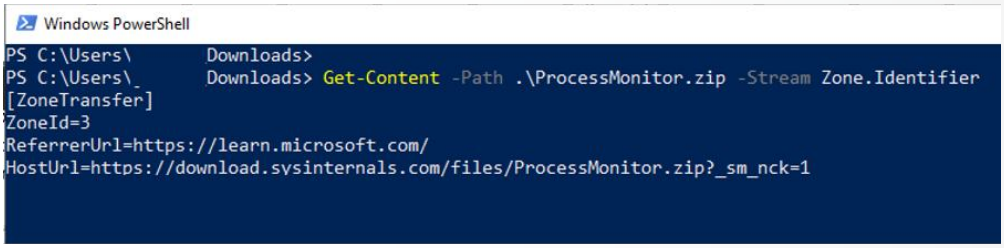


Figure 6 : Utilisation de PowerShell pour afficher la marque du Web sur un fichier téléchargé.

Cette Mark of the Web (MotW) est ensuite utilisée par Microsoft Office, Microsoft SmartScreen et d'autres outils de sécurité pour appliquer des restrictions, par exemple pour empêcher l'exécution automatique de macros potentiellement malveillantes dans un document Word.

Dans ce cas, RomCom a découvert un programme d'exécution de code à distance de type "zero-day" pour contourner les protections de Mark of the Web. Ils ont exploité une fonction de recherche de Windows pour télécharger des fichiers distants sur le système de fichiers local où, pendant un court laps de temps, ils n'ont pas été marqués avec le MotW. Les protections de la marque du web ont ainsi été contournées, ce qui a permis à l'attaquant d'exécuter des actions qui auraient normalement été interdites pour du contenu téléchargé depuis l'internet. Les auteurs de la menace ont alors été en mesure d'initier une chaîne d'événements qui a abouti à l'exécution d'un code arbitraire.

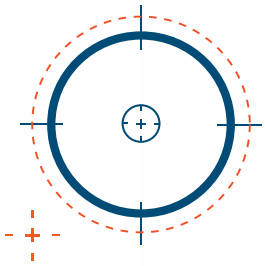
Il est intéressant de noter que la structure des documents malveillants utilisés par RomCom contient des éléments de Follina Exploit (mis en évidence dans le rapport de l'année dernière), l'analyse la reliant à CVE-2022-30190, une vulnérabilité qui a également été utilisée pour contourner les contrôles de sécurité des documents Office. Alors que Microsoft a amélioré la sécurité par défaut d'Office, les pirates ont continué à innover pour contourner les protections.

Cet exploit n'est pas le seul. En 2023, des chercheurs de Palo Alto Networks ont également découvert CVE-2023-36584, qui utilisait un vecteur d'exploitation différent pour contourner les protections MotW. Ce flux constant de vulnérabilités d'exécution de code à distance dans Office montre que, malgré les récentes améliorations de la sécurité de Microsoft, les attaquants trouvent toujours des moyens d'exécuter du code.

De nombreuses organisations qui luttent contre les vulnérabilités historiques d'Office et les fonctions de sécurité qui ne sont pas activées par défaut peuvent avoir l'impression que la bataille est perdue. Cependant, comme pour toutes les vulnérabilités liées à l'exécution de code à distance, le principe du moindre privilège est une mesure défensive essentielle.

En fin de compte, quel que soit l'exploit, la charge utile du logiciel malveillant s'exécutera dans le contexte de l'utilisateur qui a ouvert le document. Si cet utilisateur dispose de privilèges d'administrateur, l'acteur de la menace en fera de même.

Mais si vous supprimez les privilèges et mettez en place une couche de contrôle des applications, vous pouvez atténuer la menace de manière proactive, même en cas d'utilisation d'un exploit de type "zero-day".



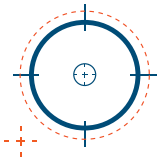
Le principe du moindre privilège est une mesure défensive essentielle. Quelle que soit la nature de l'exploit, si vous supprimez les privilèges et mettez en place une couche de contrôle des applications, vous pouvez atténuer la menace de manière proactive, même lorsqu'un exploit de type "zero-day" est utilisé.

Les organisations traversent-elles une crise d'identité ?

De plus en plus, les attaquants recentrent leurs efforts sur l'exploitation des identités plutôt que sur les vulnérabilités des logiciels Microsoft. Midnight Blizzard représente un excellent exemple de ce qui peut arriver lorsque les acteurs de menace innovent avec des tactiques d'infiltration basées sur l'identité.

Il y a quelque temps, Morey J. Haber, Chief Security Advisor chez BeyondTrust, a posé la question suivante : "Sommes-nous en train de vivre une crise d'identité ?" Le jeu de mots nous a d'abord pris au dépourvu, mais nous avons vite compris que sa question était un jeu de mots basé sur les défis croissants auxquels les organisations sont confrontées en matière de gestion et de sécurisation des identités.

En tant que Chief Security Advisor et ancien CSO et CTO, M. Morey a suivi la marée montante des menaces liées à l'identité, tout en aidant d'autres personnes à comprendre les défis complexes et le paysage des menaces. Son nouveau livre, **Identity Attack Vectors : Strategically Designing and Implementing Identity Security**, fournit une évaluation approfondie des défis liés à la mise en œuvre d'une véritable sécurité de l'identité au sein d'une organisation.



« [Votre] crise d'identité n'est pas une crise personnelle, mais décrit plutôt un problème lié à la façon dont vous gérez les identités et la sécurité des identités au sein de votre organisation . »

Morey J. Haber,
Chief Security Advisor ,
BeyondTrust

Étant donné que ce rapport est conçu pour aider les organisations à mieux comprendre le paysage des menaces autour de l'écosystème Microsoft et au-delà, il est important de répondre à cette crise d'identité et au fait que les attaquants mettent davantage l'accent sur les vecteurs d'attaque basés sur l'identité.

Comment identifier une crise d'identité dans votre écosystème Microsoft :

Questions clés basées sur les vecteurs d'attaque lié aux identités

À quoi ressemble une crise d'identité dans votre écosystème Microsoft ?

Cela ressemble à un utilisateur qui se connecte, et c'est ce qui rend les choses si difficiles. Vous pouvez disposer de systèmes entièrement corrigés et d'excellents outils de sécurité, mais si un attaquant parvient à voler des identifiants, à détourner un token de session ou de faire de l'ingénierie sociale au sein du service support, il peut être en mesure d'entrer directement dans votre environnement. Dans un monde où il est plus facile de se connecter que de pirater, l'identité devient le nouveau périmètre.

Il s'agit des vulnérabilités, des problèmes de processus et des risques associés à la relation entre l'identité et le compte.
Les risques eux-mêmes peuvent être diagnostiqués en identifiant les failles dans le processus d'adhésion, de migration et de désengagement, ainsi que dans les autorisations, droits, privilèges, rôles, authentification (comme l'authentification multifactorielle (MFA) et l'authentification unique (SSO)) et autorisation pour les identités et les comptes au repos et fonctionnant pendant l'exécution.

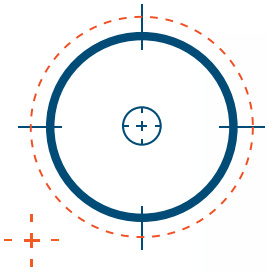
Qu'est-ce qui transforme un défi de sécurité en une crise d'identité ?

Les détections et recommandations nécessaires à la classification des risques sont généralement enfouies profondément dans les données. Sans une approche clinique du problème, les symptômes passent souvent inaperçus, à moins que un professionnel de la sécurité ne les recherche spécifiquement.

L'état d'esprit de nombreuses équipes de sécurité se concentrent désormais sur la traque et la détection des menaces alors qu'en réalité, il est nécessaire de devenir plus proactif. En matière de crise d'identité, les vulnérabilités ne sont peut-être pas des failles dans le code sous-jacent.

La vulnérabilité pourrait être une mauvaise configuration dans l'Active Directory qui permet à n'importe quel utilisateur d'élever ses privilèges. Il pourrait également s'agir d'une combinaison de rôles Entra ID obscurs qui permettent à un attaquant d'ajouter des identifiants à une application OAuth privilégiée pouvant accéder aux emails des entreprises.

> « La prévention est essentielle, mais on ne peut jamais tout éviter. Vous avez également besoin d'une détection."
>
> **Jay Beale, PDG, CTO, InGuardians, Inc.**



Les attaquants réfléchissent à l'aide de graphiques complexes pour naviguer dans les systèmes Microsoft.

> **Il existe un dicton assez célèbre en matière de sécurité :**
> "Les défenseurs pensent en termes de listes. Les attaquants pensent en termes de graphiques. Tant que cela est vrai, les attaquants gagnent."
>
> John Lambert,
> Corporate Vice President, Security Fellow,
> Microsoft Security Research.

L'idée est qu'un défenseur réfléchit en listes cloisonnées:

- Défenseur A pense à l'Active Directory,
- Defender B pense à Windows Desktop AV,
- Defender C pense aux serveurs Windows, etc.

L'attaquant, quant à lui, réfléchit à un graphique ou à une série de connexions entre les comptes et les systèmes qu'il peut utiliser pour atteindre son objectif. Ils exploitent le manque de visibilité entre ces systèmes disparates (les listes du défenseur) pour se déplacer latéralement et infliger des dégâts. Cela pourrait signifier démarrer sur Windows Desktop avec un utilisateur privilégié d'administrateur local, puis utiliser cet accès pour capturer un compte de domaine privilégié et pivoter sur un serveur.

> **Nous devons être capables de penser sous forme de graphiques**, tout comme le font les attaquants. Si nous pouvons obtenir une visibilité plus globale de tous les comptes, privilèges et accès dans notre environnement, nous pourrons alors commencer à sortir de nos silos et de nos listes pour voir ce que les attaquants voient et ce qu'ils peuvent exploiter dans nos environnements.
>
> Nous pouvons comprendre et corriger les chemins vers les privilèges, les vulnérabilités et les erreurs de configuration. Bien que cela soit plus facile à dire qu'à faire, il est essentiel de pouvoir faire pencher la balance en faveur des défenseurs et de garder une longueur d'avance sur les menaces.

En tant qu'industrie, nous devons commencer à réfléchir de manière plus globale aux privilèges, à l'hygiène de l'identité et à la détection des menaces d'identité.

Les principaux messages, qui ont résonné à travers ce rapport des 11 dernières années – application du moindre privilège, renforcement des configurations et importance des correctifs – représentent certaines des stratégies de base nécessaires pour se défendre contre les cybermenaces. Ces messages fondamentaux s'appliquent également à la crise d'identité. Peu importe qu'un compte soit compromis via un piratage de session dans le cloud ou une vulnérabilité exploitée sur un endpoint : moins l'utilisateur compromis dispose de privilèges et d'accès, plus le risque est réduit.

Voyons comment Microsoft a été impacté par sa propre crise d'identité en 2023.

Microsoft mis à l'épreuve par Midnight Blizzard

Les attaquants ont orchestré une attaque magistrale, en tirant parti de tactiques d'infiltration basées sur l'identité, des privilèges et des accès souvent inaperçus pour se frayer un chemin à travers les systèmes de Microsoft.

L'attaque Midnight Blizzard a illustré à quel point il est plus facile pour les attaquants de se connecter avec un compte volé que de pirater en exploitant une vulnérabilité.

Un excellent exemple d'attaque moderne basée sur l'identité s'est produit lorsque Microsoft a été ciblé par les acteurs de la menace connus sous le nom de Midnight Blizzard (également Cozy Bear et APT29). Cette attaque ne semble pas avoir impliqué l'une des vulnérabilités logicielles que nous couvrons traditionnellement dans ce rapport. Il s'agissait plutôt d'un cours magistral où **les attaquants pensaient en termes de graphiques** et utilisaient des privilèges et des accès souvent inaperçus entre les comptes et les systèmes pour se frayer un chemin à travers les systèmes de Microsoft.

L'attaque a commencé en 2023, lorsqu'un compte dans un environnement de test hors production a fait l'objet d'une attaque par pulvérisation de mot de passe. Malheureusement, le compte Entra ID ciblé ne disposait pas d'une authentification multifactorielle (MFA). Cela signifie qu'une fois que les attaquants ont réussi à deviner le mot de passe, ils ont eu accès au compte.

Il apparaît que le compte compromis, bien qu'il ne soit pas directement surprivilégié, avait la capacité de créer de nouveaux secrets pour les applications OAuth dans l'environnement de test. À ce stade, l'attaquant aurait dû être limité à l'environnement de test, mais ce n'était pas le cas. Microsoft a déclaré que, dans l'environnement de test, il y avait une "ancienne application OAuth de test qui avait un accès élevé à l'environnement de l'entreprise Microsoft". Cela signifie que les attaquants avaient la possibilité d'ajouter des secrets, de s'authentifier en tant qu'application de test privilégiée disposant d'un accès élevé à l'environnement de l'entreprise, puis d'exécuter des commandes.

Avec ce niveau d'accès étendu, les attaquants ont pu créer une nouvelle application OAuth malveillante et lui accorder l'autorisation "full_access_as_app" Microsoft 365 Exchange Online pour l'environnement de l'entreprise. Cette autorisation a permis aux attaquants d'accéder aux boîtes mails des cadres supérieurs à l'aide d'identifiants attribuées à leur application OAuth malveillante.

Cette attaque est un bon exemple de la façon dont le paysage des menaces évolue vers un point de basculement : **il devient plus facile pour les attaquants de se connecter avec un compte volé que de pirater en exploitant une vulnérabilité.**

Comme nous l'avons montré au cours des 11 années d'existence de ce rapport, le paysage est en constante évolution.

Avec les investissements de Microsoft dans la sécurisation de ses logiciels et la réduction du nombre de vulnérabilités critiques, combinés à la poussée vers le cloud rendant les données et les systèmes accessibles depuis n'importe quel réseau, **nous ne pouvons que supposer que le volume et la sophistication des menaces de sécurité des identités vont augmenter considérablement au cours de la prochaine décennie.**

> "Midnight Blizzard est un autre exemple de l'adage populaire : "Les attaquants ne s'introduisent pas par effraction, ils se connectent"."
>
> **Jay Beale, PDG, CTO, InGuardians, Inc.**

Que disent les experts ?

Paula Januszkiewicz

PDG
CQURE

Nous assistons tous à une évolution de l'importance de la cybersécurité dans la vie quotidienne. Pendant longtemps, elle a été une préoccupation de niche réservée aux passionnés de technologie. Aujourd'hui, elle est devenue un aspect essentiel de la réalité quotidienne des particuliers et des entreprises. Alors que le monde devient de plus en plus digital, les enjeux liés à la protection de nos données et de notre vie privée sont plus importants que jamais. Les conclusions du Microsoft Vulnerabilities Report 2024 de BeyondTrust nous rappellent les défis permanents auxquels nous sommes confrontés.

Suite du commentaire de Paula à la page suivante >

2023 a été l'année de l'IA, de l'IA générative et de l'automatisation, qui continueront de révolutionner notre approche de la cybersécurité dans les années à venir. Ces technologies offrent un potentiel incroyable pour détecter et atténuer les menaces, soutenir nos stratégies de défense et rendre le travail des équipes SecOps plus gérable. Cependant, ils introduisent également de nouveaux défis, tels que les deepfakes et les campagnes de désinformation sophistiquées. L'IA est rapidement devenue une arme à double tranchant : un outil puissant au service des deux côtés.

Ce rapport sur les vulnérabilités Microsoft met en lumière une image nuancée de l'état actuel des vulnérabilités. Sur une note positive, les vulnérabilités critiques ont connu une légère diminution, poursuivant une tendance encourageante. En outre, le nombre de vulnérabilités d'élévation de privilèges (catégorie de vulnérabilité principale) a considérablement diminué, probablement grâce au travail sur les vulnérabilités Azure et Windows Server. Pourtant, le nombre global de vulnérabilités au sein de l'écosystème de Microsoft reste stable, signe inquiétant que, malgré tous les efforts et investissements, le paysage des menaces est loin de diminuer. L'augmentation marquée des vulnérabilités d'usurpation d'identité est particulièrement frappante, soulignant le besoin constant de vigilance.

Il est essentiel d'affiner notre approche de la cybersécurité. Il s'agit notamment de contrôler plus strictement les privilèges, de renforcer les protocoles de sécurité et d'adapter nos défenses aux caractéristiques de nos environnements. La clé est de rester informé sur les menaces émergentes, de déployer des mécanismes de détection et de réponse efficaces, d'effectuer régulièrement des audits et des tests de pénétration, et de revoir et tester en permanence nos plans de réponse aux incidents. Ces principes résonnent profondément avec nos propres expériences, renforçant leur rôle essentiel dans le maintien d'un cadre de cybersécurité solide.

Nous ne devons cependant pas oublier que l'élément humain reste au cœur de la cybersécurité. Les défenses technologiques les plus avancées peuvent être compromises par une simple erreur humaine. Le présent rapport fait état d'un changement en cours : il devient plus facile de voler des identités que d'exploiter une vulnérabilité. Par conséquent, les attaques basées sur l'identité deviendront probablement encore plus courantes dans un avenir proche.

Il est donc essentiel de promouvoir une culture de la sensibilisation et de l'éducation auprès de tous les utilisateurs. Contrairement au piratage informatique, qui est souvent un travail solitaire, la cybersécurité est par nature un effort de collaboration. Ce point de vue, repris dans le rapport, souligne l'importance d'une approche de la cybersécurité centrée sur les personnes.

En réfléchissant aux informations recueillies dans le rapport de BeyondTrust, il est clair que le chemin à parcourir en 2024 nous obligera à adapter et à repenser nos stratégies de cybersécurité. Les adversaires devenant de plus en plus sophistiqués, il sera vital d'intégrer la cybersécurité plus profondément dans nos routines quotidiennes et nos activités commerciales. La clé pour naviguer dans l'avenir sera une approche équilibrée qui combine l'innovation technologique avec un engagement fort en faveur de l'éducation et de la coopération.

Mon conseil ? Rester vigilant, accepter le changement, apprendre constamment de la communauté et ne pas oublier de rendre la pareille. C'est ainsi que nous pourrons garantir un avenir plus sûr pour tous.

David Morimanno

Directeur des technologies de gestion des identités et des accès, Integral Partners, une société Xalient

Les conclusions du rapport de cette année sur les vulnérabilités de Microsoft confirment ce que nous avons observé dans le paysage contemporain de la cybersécurité. Alors que les cybercriminels se concentrent de plus en plus sur les vulnérabilités centrées sur l'identité, un solide programme de gestion des identités et des accès joue un rôle essentiel dans l'atténuation de l'évolution des menaces. Cela est particulièrement vrai pour les menaces centrées sur les vulnérabilités identitaires au sein de l'écosystème Microsoft, facilitées par l'expansion des plateformes en nuage telles qu'Azure et Microsoft 365. Les systèmes complexes et interconnectés introduisent des vulnérabilités imprévues, ce qui nécessite une approche proactive des mesures de sécurité centrées sur l'identité.

La mise en œuvre des principes de confiance zéro est devenue une priorité pour de nombreuses organisations avec lesquelles nous travaillons, tout comme la construction d'une structure d'identité. Une structure d'identité est un paradigme pour un ensemble complet de services d'identité, offrant les capacités nécessaires pour fournir un accès transparent et contrôlé à tous les services. L'intégration de la gestion des accès privilégiés dans la structure d'identité plus large est impérative pour renforcer les mesures de sécurité et éviter les cyberattaques potentielles.

Pourquoi le nombre de vulnérabilités signalées est-il resté stable ?

Dans ce rapport, le nombre de vulnérabilités Microsoft est resté relativement stable. Pourquoi donc?. Les efforts de Microsoft pour corriger rapidement les vulnérabilités connues pourraient contrecarrer la découverte de nouvelles vulnérabilités en réduisant la fenêtre d'opportunité permettant aux attaquants d'exploiter les vulnérabilités. De plus, à mesure que la base de code MS mûrit, de nouvelles vulnérabilités pourraient être introduites à un rythme plus lent. Une autre possibilité est que les produits Microsoft s'appuient souvent sur des bibliothèques et des composants tiers, ce qui pourrait introduire des vulnérabilités qui ne sont pas directement imputables au code de Microsoft.

L'importance du PAM et sa contribution à la structure de l'identité

L'incident CVE-2023-23397 souligne les dangers de la confiance dans les mots de passe et des contrôles d'accès inadéquats. L'exploit "zéro-clic" ne nécessitait pas d'interaction de la part de l'utilisateur, ce qui a permis de compromettre un système vulnérable par le biais d'un email non ouvert ! De telles attaques soulignent la nécessité d'une authentification multifactorielle (MFA), d'une segmentation, d'un moindre privilège et de l'application de correctifs en temps opportun pour atténuer des risques similaires. Le PAM joue évidemment un rôle crucial dans l'atténuation des risques en tant qu'élément d'un programme holistique centré sur l'identité qui renforce votre structure d'identité plus large, englobant l'AGI, la gestion des accès, les services d'annuaire et la gestion des habilitations de l'infrastructure en nuage (CIEM).

Suite du commentaire de David à la page suivante >

L'un des nombreux outils que nous utilisons dans notre pratique de conseil pour aider les organisations à traiter efficacement les risques liés à l'identité est une liste de contrôle complète d'évaluation des risques liés à l'identité, qui englobe des facettes telles que la gouvernance, la gestion du cycle de vie, l'accès privilégié et les identités machine.

Nous insistons également sur la nécessité de tirer parti de l'intelligence artificielle (IA) dans la mesure du possible. L'avenir de la sécurité centrée sur l'identité s'appuiera sans aucun doute sur des technologies avancées telles que l'intelligence artificielle et l'analyse comportementale pour détecter et répondre aux menaces en temps réel, en veillant à ce que les organisations restent résilientes face à des cyber-risques en constante évolution.

Greg van der Gaast

Directeur général
Sequoia Consulting
sequoia-consulting.co.royaume-uni
greg@sequoia-consulting.co.royaume-uni.

Greg van der Gaast est directeur général de Sequoia Consulting, une société de conseil en sécurité spécialisée dans la résolution des problèmes liés aux activités et aux processus afin de réduire les problèmes de sécurité.

"La valeur des vulnérabilités"

J'ai pensé pouvoir apporter des conseils pratiques sur la façon d'exploiter vos vulnérabilités de manière plus stratégique et d'examiner des choses plus importantes qu'une note CVSS.

Si nous voulons progresser dans l'amélioration de la posture de sécurité de notre organisation, plutôt que de lutter contre les incendies, nous devons moins nous préoccuper des vulnérabilités que nous avons et davantage des raisons pour lesquelles nous les avons.

Par exemple, l'hypothétique CVE de score CVSS 9,8 qui est apparu hier ne me préoccupe pas vraiment. Mon processus d'application de correctifs devrait gérer cette situation de manière opérationnelle dans les 24 à 48 heures.

Si ce n'est pas le cas pour vous, je vous suggère de consacrer plus de temps à la maturation de votre programme de correctifs. S'il y a des raisons pour lesquelles nous ne pouvons pas patcher, nous devrions nous demander pourquoi ces raisons existent, si elles sont vraiment nécessaires et ce que nous pouvons faire pour changer cela.

Les CVE les plus récents, les plus importants, les plus effrayants ne m'inquiètent pas. Ce qui m'inquiète, c'est la vulnérabilité "à faible risque" vieille de deux ans. Sa présence me dit quelque chose.

Suite du commentaire de Greg à la page suivante >

S'il est présent depuis le début, il y a potentiellement quelque chose qui ne va pas du tout avec mes correctifs opérationnels.

Si elle vient d'apparaître, est-ce que j'ai un problème avec la façon dont les nouveaux systèmes sont construits, ou avec la façon dont il est possible d'installer d'anciens logiciels vulnérables sur des systèmes existants ? Peut-être que ces processus sont corrects, mais qu'ils sont contournés par un problème d'approvisionnement ou d'informatique parallèle ?

Ce sont ces problèmes dans nos processus qui créent l'accumulation de risques qui contribueront à une éventuelle violation. S'attaquer à ces problèmes permet de réduire de manière cumulative et durable les risques encourus par l'entreprise au fil du temps, ce qui signifie que nous avons de moins en moins de soucis à nous faire.

Il est étonnamment facile de trouver ces problèmes : nos vulnérabilités nous indiquent exactement où se trouvent ces problèmes.

Les vulnérabilités que nous avons corrigées dans le passé - sans tenir compte de leur origine - peuvent avoir été une occasion manquée de trouver la cause première de ce qui nous fera subir une violation à l'avenir.

Terry Cutler

Hacker éthique et fondateur, Cyology Labs

Protéger votre entreprise : conseils d'un hacker professionnel

En réalité, que vous soyez un entrepreneur individuel ou que vous gériez une entreprise florissante, il est essentiel de reconnaître que les cybermenaces peuvent viser n'importe qui. À mesure que les cybermenaces gagnent en complexité, aucune entité n'est à l'abri. Les tendances récentes révèlent une augmentation significative des incidents qui touchent les collectivités locales, les municipalités et les entreprises et qui entraînent des pertes financières considérables.

Comment opèrent les hackers : le manuel de l'initié

Les pirates informatiques utilisent généralement une approche d'attaque structurée qui comporte toujours quelques phases. Ils commencent par la reconnaissance, en recueillant des informations numériques. Ensuite, ils effectuent des balayages pour trouver des vulnérabilités, comme un cambrioleur qui vérifie s'il y a des portes non verrouillées.

Une fois qu'ils ont trouvé un point d'entrée, ils l'exploitent pour obtenir et maintenir l'accès, tout en couvrant leurs traces. Enfin, ils perturbent systématiquement les systèmes.

Le commentaire de Terry continue à la page suivante >

Le plan d'action pour la cyber-résilience

La mise en œuvre de pratiques de base en matière de cybersécurité peut prévenir de nombreuses attaques. Des actions simples, telles que la mise à jour de vos logiciels, l'application des correctifs publiés par Microsoft, la prudence face aux escroqueries par hameçonnage et l'utilisation de mots de passe forts et uniques avec une vérification en deux étapes, sont essentielles.
Comme l'a continuellement montré le rapport de BeyondTrust sur les vulnérabilités de Microsoft, la suppression des droits d'administration superflus et l'application du principe du moindre privilège constituent une étape essentielle de ce processus. C'est comme verrouiller les portes et les fenêtres : simple, mais efficace pour empêcher les intrus d'entrer et ne permettre l'accès qu'à la bonne personne au bon moment.

Il est essentiel de procéder à une cyber-évaluation complète afin de détecter les éventuelles vulnérabilités.

Pour protéger efficacement votre réseau, vos endpoints et votre infrastructure cloud, adoptez des stratégies avancées telles que l'authentification multifactorielle (MFA), le chiffrement, la sécurité de l'identité et de l'accès et les technologies modernes de cyberdéfense. Personnalisez vos défenses en fonction de vos risques spécifiques et soyez prêt à vous adapter pour suivre l'évolution des menaces.

Sami Laiho

MVP du système d'exploitation Windows
Directeur de recherche / Fondateur, Adminize

LinkedIn
X (anciennement Twitter)

Comme l'indique le rapport 2024 sur les vulnérabilités de Microsoft, "le nombre total de vulnérabilités continue de se maintenir pendant trois ans à un niveau proche des chiffres les plus élevés jamais atteints". Nous avons cessé de tester les mises à jour des définitions anti-programmes malveillants avant de les déployer lorsqu'elles étaient moins nombreuses, car les mises à jour de Windows sont désormais mensuelles. Ont-elles parfois échoué ? Oui. Avons-nous arrêté les mises à jour ? Non. Je pense que chacun d'entre nous choisira une indisponibilité potentielle de deux heures à laquelle il est préparé et qu'il maîtrise, plutôt qu'une indisponibilité de trois mois contrôlée par une tierce partie.

J'ai une règle avec mes clients : les correctifs critiques ou les correctifs pour tout ce qui a une IP publique seront corrigés les jours 1 à 3. Tout le reste est patché dès que possible - et pour vos pare-feu et passerelles VPN, vous patchez tous les jours qui commencent par la lettre T : mardi (Tuesday), jeudi (Thursday), aujourd'hui (Today) et demain (Tomorrow). Avec le principe du moindre privilège, nous pouvons encore atténuer environ la moitié de toutes les vulnérabilités critiques, c'est donc toujours l'une des lois immuables de la sécurité Windows - comme le dit le guide de l'utilisateur NT 3.1 de 1993, il n'y a pas de sécurité dans Windows si vous vous connectez en tant qu'administrateur.

Heureusement, le Zero Trust (aussi mauvais que soit son nom) a fait remonter le principe du moindre privilège à la surface. Les acteurs malveillants ont besoin des droits administrateur pour exécuter les outils vraiment dangereux, et c'est donc ce qu'ils recherchent. Comme le montre le rapport sur les vulnérabilités de Microsoft, "l'élévation des privilèges représentait 40 % (490) du total des vulnérabilités en 2023".

« Puisque les privilèges sont ce que veulent les acteurs de menace, notre tâche principale devrait être de nous assurer qu'ils ne les obtiennent pas. »

Sami Laiho, MVP Du Système D'exploitation Windows, Directeur De Recherche/Fondateur, Truesec Finlande

Eliza-May Austin

PDG
th4ts3cur1ty.entreprise

Gestion des vulnérabilités, élévation de privilèges et identité comme surface d'attaque

Les résultats du rapport 2024 sur les vulnérabilités de Microsoft montrent que la phase d'élévation des privilèges (PrivEsc) continue de dominer en tant que tactique offensive efficace. Le PrivEsc, une phase d'attaque nécessaire et requise, deviendra le centre d'intérêt des acteurs de la menace, plus encore que la pénétration du périmètre.

La prévisibilité d'un périmètre structuré au sens classique s'amenuise, les entreprises de toutes tailles visant à réduire leurs architectures classiques en faveur de l'approche "sans serveur". L'identité de l'utilisateur deviendra la surface d'attaque privilégiée par rapport au périmètre traditionnel. Les acteurs de la menace s'attaqueront à l'identité (le compte) plutôt qu'à la compromission du système, car les entreprises s'alignent de plus en plus sur la confiance zéro en tant qu'approche architecturée. Cela signifie que la confiance zéro est, en théorie, contournée.

La concentration sur le titulaire du compte entraînera une augmentation du besoin de structures et de capacités en criminalistique numérique et de réponse aux incidents (DFIR). Il est essentiel de reconnaître la grande quantité de données collectées par les adversaires nationaux. Ces données pourraient être croisées avec des données d'entreprise et des informations personnelles, ce qui permettrait aux adversaires d'identifier les vulnérabilités spécifiques du titulaire du compte. Cela facilite à son tour les attaques très ciblées sur les identités des individus. Ces attaques peuvent exploiter efficacement les faiblesses du titulaire du compte pour obtenir un accès là où une attaque de type "zero day" aurait autrement été nécessaire. Le développement d'attaques personnalisées et inédites (zero days) coûte du temps, de l'argent et des ressources humaines, et si un groupe de menace peut éviter d'en lancer une (de l'utiliser) en se concentrant plutôt sur les identités, il le fera. Ils chercheront toujours le fruit le plus bas et attaqueront les utilisateurs qui commettent des erreurs ou les systèmes qui ne sont pas bien défendus.

Suite du commentaire d'Eliza-May à la page suivante >

L'attaque des comptes conduira sans aucun doute à des attaques plus complexes et, honnêtement, plus impressionnantes. Nous pourrions même voir ce phénomène s'étendre davantage, les attaques évoluant vers des formes d'attaques plus distantes, de fournisseur à fournisseur, de fournisseur à cible, et ainsi de suite. Comme la dépendance à l'égard du SaaS continue de croître pour tenter de contourner cette expansion, nous remarquerons une augmentation de ce que j'aime appeler les "Jackpotattacks", comme celles de SolarWinds et FireEye.

Si l'on se réfère au rapport de Microsoft sur les vulnérabilités, il est essentiel de donner la priorité à la gestion des vulnérabilités et d'apprendre aux entreprises à faire la distinction entre l'analyse et la gestion. L'acquisition de licences d'analyse est simple, mais la mise en place d'un processus interne d'identification, de hiérarchisation, de remédiation et de test des mesures d'atténuation reste un défi constant, en raison des dépendances entre départements et du manque d'indicateurs de performance mesurant la réduction de l'exposition aux vulnérabilités.

Marc Maiffret

CTO
BeyondTrust

En tant que CTO chez BeyondTrust et fan de Spinal Tap, je suis ravi de voir ce rapport passer à la vitesse supérieure cette année. Ce rapport continue de souligner la nécessité de continuer à améliorer la sécurité, non seulement chez Microsoft, mais aussi pour toutes les organisations qui cherchent à mieux gérer les cyber-risques dans le contexte d'un paysage de menaces en constante évolution.

Bien que le nombre de vulnérabilités critiques de Microsoft atteigne un niveau historiquement bas, le rapport contient quelques bons exemples de raisons de ne pas se reposer sur ses lauriers en matière de vulnérabilités. Malgré des avancées majeures dans la sécurité globale de l'écosystème Microsoft, la CVE-2023-23397 permettant la capture des hachages NTLM via Outlook, et la CVE-2023-36884 permettant le contournement de Mark of the Web, nous montrent toutes deux qu'il existe encore de nombreuses surfaces d'attaque qui ne demandent qu'à être trouvées et exploitées.

La domination continue de l'élévation des privilèges en tant que catégorie de vulnérabilité la plus courante et la crise d'identité mise en évidence à la fin du rapport soulignent l'importance des privilèges et du concept de sécurité intemporel du moindre privilège.

Suite du commentaire de Marc à la page suivante >

Au début de ma carrière, j'ai eu la chance de découvrir les Rainbow Books, une série de normes de sécurité informatique publiées par le ministère américain de la défense dans les années 1980 et 1990. Ces livres, et les concepts de surface d'attaque et de moindre privilège qui y sont décrits, sont tout aussi pertinents pour les défis que nous rencontrons aujourd'hui qu'ils l'étaient il y a plus de 30 ans, lorsque les livres ont été publiés pour la première fois.

> "Moindre de privilèges : ce principe exige que chaque sujet d'un système se voie accorder l'ensemble de privilèges le plus restrictif nécessaire à l'exécution des tâches autorisées. L'application de ce principe limite les dommages pouvant résulter d'un accident, d'une erreur ou d'une utilisation non autorisée".
>
> **A Guide To Understanding Discretionary Access Control In Trusted Systems, 1987**

Quand je pense à la sécurité des identités aujourd'hui, ce ne sont pas les identités elles-mêmes qui ont de la valeur, ce sont les privilèges liés ces identités qui ont de la valeur et qui en font une cible. C'est pourquoi les acteurs de la menace recherchent les vulnérabilités liées à l'élévation des privilèges et les identités ayant accès aux privilèges. C'est la raison our laquelle les correctifs et le moindre privilège restent parmi les meilleurs moyens de réduire votre surface d'attaque. C'est également pour cela que BeyondTrust s'est donné pour mission de fournir le plus large niveau de visibilité et de protection des privilèges.

L'attaque Midnight Blizzard, mentionnée dans le rapport de cette année, illustre parfaitement le paysage moderne des menaces contre les identités. Dans cet esprit, je vais lancer un défi aux auteurs de ce rapport pour l'année prochaine : aller au-delà des vulnérabilités des logiciels Microsoft et analyser certaines des erreurs de configuration courantes ou des paramètres par défaut faibles qui introduisent des vulnérabilités de configuration dans l'écosystème Microsoft, permettant ainsi aux attaquants d'accéder à des privilèges et d'exploiter les systèmes.

Restez en sécurité ! .

Dr Jessica Barker MBE

Co-fondateur, Cygenta
Auteur de Piratage : les secrets des cyberattaques
LinkedIn
X (anciennement Twitter)

Les données de cette année continuent de montrer que le travail dans le domaine de la sécurité est payant. En travaillant dans ce domaine, nous avons parfois l'impression de ne pas progresser, voire de reculer, car les attaquants gagnent beaucoup plus souvent que nous.

Nous devons rechercher les failles, c'est-à-dire la seule fois où quelque chose ne va pas plutôt que les 100 fois où tout va bien. Et avec un paysage de menaces en constante évolution, nous pouvons avoir l'impression de nager à contre-courant.

C'est pourquoi nous devons avoir une vue d'ensemble, reconnaître que les problèmes complexes de la cybersécurité ne seront pas résolus du jour au lendemain et faire le point sur les progrès accomplis en cours de route.

Il n'est pas surprenant que l'escalade des privilèges reste la catégorie de vulnérabilité numéro un dans le rapport de cette année. Cependant, même cette catégorie de vulnérabilité, la plus importante, montre une nette amélioration. Cela nous rappelle que nous ne pouvons pas tout régler du jour au lendemain, mais que nous pouvons progresser, même dans les domaines difficiles.

Le rapport de cette année souligne que les attaquants "pensent en graphiques". En matière de cybersécurité, nous devons également penser en termes de systèmes. Lorsqu'il s'agit d'ingénierie sociale et de l'aspect humain de la sécurité, il peut être facile de se concentrer sur ce que l'on appelle l'erreur humaine. Cependant, si nous nous concentrons uniquement sur l'individu, nous passons à côté de la cible.

Nous devons plutôt nous pencher sur les systèmes dans lesquels les gens opèrent, en réduisant la charge pour les utilisateurs finaux. Les réseaux segmentés, le moindre privilège, l'authentification multifactorielle et la gestion des vulnérabilités sont des éléments fondamentaux, étayés par un système de sécurité sain.

Ce rapport souligne également l'importance de l'identité. Avec l'essor de l'IA générative et de la technologie deepfake utilisée dans les attaques d'ingénierie sociale, la gestion de l'identité va devenir une question encore plus pressante. Il est plus que jamais crucial de sensibiliser aux menaces, tout en faisant tout ce qui est en notre pouvoir pour réduire les frictions en matière de sécurité, en donnant aux gens les moyens d'adopter des comportements sécurisés dans le cadre d'une culture de la sécurité positive et proactive.

Atténuer les risques liés à l'écosystème logiciel Microsoft et améliorer la cyber-résilience

Ensemble, les stratégies de sécurité suivantes offrent une protection en profondeur très efficace contre les exploits de vulnérabilité Microsoft ainsi que les attaques basées sur l'identité :

1. **Appliquer le moindre privilège en supprimant les droits administrateurs locaux :** Il est essentiel de maintenir une stratégie solide de gestion des accès privilégiés pour supprimer et sécuriser les privilèges dans un environnement afin d'éviter qu'ils ne tombent entre les mains d'un attaquant. Cette approche proactive peut fournir une protection très efficace, même en l'absence de correctifs. La suppression des droits d'administrateur locaux et le contrôle de l'exécution ont historiquement atténué 75 % des vulnérabilités critiques de Microsoft, comme nous l'avons démontré dans les rapports précédents lorsque Microsoft a mis à disposition des données plus spécifiques sur les privilèges. Ce chiffre de 75 % indique que, sans droits d'administrateur, la vulnérabilité ne peut pas être exploitée, même si elle n'est pas corrigée. L'approche du moindre privilège, qui est également un principe fondamental des modèles de sécurité "zéro confiance", peut contribuer à briser plusieurs points de la chaîne d'attaque - du détournement de compte au mouvement latéral, en passant par l'escalade des privilèges, et bien plus encore.

2. **Suivez les protocoles de renforcement de la sécurité, tels que l'application de correctifs :** Assurez-vous toujours que votre système d'exploitation et vos logiciels tiers sont à jour et que vous n'utilisez pas de logiciel en fin de vie dans votre environnement. De plus, supprimez les privilèges, accès et comptes inutiles pour réduire davantage la surface de risque. Gardez à l'esprit que l'application le plus tôt possible de correctifs peut également vous aider à empêcher qu'une vulnérabilité apparemment anodine ne se transforme en une menace plus importante.

3. **Voies d'accès à distance sécurisées :** le protocole RDP (Remote Desktop Protocol) de Microsoft, ainsi que les VPN et de nombreuses autres technologies d'accès à distance courantes, sont de plus en plus étendus au-delà de leurs cas d'usage appropriés, ce qui entraîne des risques de sécurité et de violations. Les ransomwares utilisent souvent le RDP comme point d'entrée. Assurez-vous que le RDP n'est pas exposé à Internet. Ne laissez pas les VPN et le BYOD se mélanger. Remplacez les VPN ou améliorez-les avec des contrôles de sécurité Zero Trust pour les cas d'usages d'accès fournisseur et d'accès privilégié.

4. **Adaptez la gestion des vulnérabilités à votre propre environnement :** Il est essentiel de rechercher, de hiérarchiser et de déterminer un chemin de remédiation pour toutes les vulnérabilités. Sans le contexte des modèles de menace de votre propre organisation, vous ne pouvez pas comprendre pleinement comment hiérarchiser les correctifs et/ou utiliser d'autres contrôles et mesures d'atténuation de renforcement de la sécurité. Ce qui est considéré comme un correctif critique pour une organisation peut ne pas l'être pour une autre. Tirez parti de votre contexte commercial pour créer la stratégie de gestion des vulnérabilités qui répond le mieux à vos risques.

5. **Rester vigilant face aux menaces émergentes :** Comprendre les menaces contribue grandement à prendre des décisions plus éclairées et à assurer votre sécurité. La dernière décennie a marqué le début de changements considérables dans le paysage des menaces Microsoft. Avec le développement et le déploiement rapides de l'IA, nous assisterons probablement à de nombreux changements significatifs dans les menaces au cours de la prochaine décennie et au-delà.

6. **Mettre en œuvre la détection et la réponse aux menaces d'identité (ITDR) :** Les organisations doivent apporter des modifications et des corrections proactives à leur posture de sécurité pour empêcher les menaces de prendre le pied, et elles doivent également orchestrer une intervention rapide pour réponse à toute attaque. L'ITDR, ou essentiellement défense d'identité en profondeur, est une approche multidisciplinaire qui vise à intégrer des capacités de visibilité globale sur la sécurité des identités, de détection des menaces, d'enquête et de réponse. Cela commence par une visibilité complète sur la sécurité des identités dans tous les magasins d'identités d'entreprise (Active Directory, Entra ID, Okta, Ping, etc.). À partir de là, les organisations peuvent mieux comprendre les chemins d'attaque qui peuvent opérer à travers ces identités et les étapes nécessaires pour améliorer leur posture ou déjouer une attaque.

Comment BeyondTrust atténue les vulnérabilités traditionnelles et les risques modernes basés sur l'identité

BeyondTrust combine une gestion complète des accès à privilèges, ainsi que des fonctionnalités CIEM et ITDR, pour atténuer les vulnérabilités de Microsoft et protéger l'ensemble de l'infrastructure d'identité, d'Active Directory à Entra ID et au-delà.

Les clients s'appuient sur les solutions BeyondTrust pour :

- Supprimer les droits administrateur et mettre en œuvre un véritable modèle de moindre privilège conforme aux principes du Zero Trust.
- Sécurisez les voies et l'infrastructure d'accès à distance en garantissant que tous les accès des employés, des fournisseurs et autres sont granulaires, contrôlé et audité.
- Empêcher le piratage de compte et l'élévation des privilèges en gérant de manière sécurisée toutes les identitfiants privilégiés humains et machines, les secrets DevOps, clés SSH et mots de passe des employés qui touchent l'entreprise.
- Gérez, surveillez et auditer chaque session privilégiée, aussi éphémère soit-elle.
- Gérer et réduire efficacement l'ensemble de la surface d'attaque de l'identité, couvrant Microsoft et d'autres acteurs d'identités (Okta, Ping, etc.).
- Détecter intelligemment et neutraliser les attaques d'identité avec rapidité et précision.
- Répondre aux exigences rigoureuses de conformité et d'investigation en fournissant des rapports sur toutes les activités privilégiées et à d'autres informations sur l'identité.
- Conformez-vous pour la cyberassurance en respectant plusieurs contrôles de sécurité clés exigés par les fournisseurs de cyberassurance.

Avec BeyondTrust, les organisations bénéficient du meilleur des deux mondes : la protection proactive la plus avancée contre les menaces externes (ransomware, logiciels malveillants, etc.) et les menaces internes, ainsi que des capacités de détection et de réponse pour arrêter les attaques en cours. **En savoir plus.**

> "Les identifiants privilégiés de longue durée apparaissent dans de nombreux rapports de violation. Nous devons mieux les gérer et les éliminer là où nous le pouvons."
>
> **Jay Beale, PDG, CTO, InGuardians, Inc.**

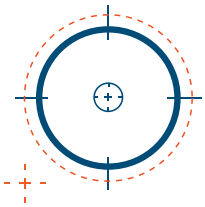
Conclusion

Bien que le nombre total de vulnérabilités Microsoft reste proche de son niveau record, elles ont plus ou moins stagné depuis 2020. Au cours de cette même période, le nombre de vulnérabilités critiques a poursuivi sa tendance à la baisse.

La stabilisation du nombre global de vulnérabilités reflète les investissements en matière de sécurité et l'attention accordée par Microsoft. Pourtant, comme l'ont montré certaines vulnérabilités critiques et de nouvelles tactiques de menace innovantes mises à profit l'année dernière, ce n'est pas le moment de faire preuve de complaisance. Il existe de nombreuses vulnérabilités, y compris des systèmes non corrigés avec des vulnérabilités connues, qui permettent aux acteurs malveillants de lancer trop facilement une attaque réussie.

De plus, à mesure que le parc technologique de Microsoft continue de s'étendre, il apportera de nouvelles surfaces d'attaque et de nouveaux vecteurs de menaces potentiels. Les vulnérabilités continueront également d'apparaître, et les acteurs de la menace continueront de réfléchir par graphiques pour naviguer dans des voies innovantes à travers les systèmes Microsoft.

Comme nous l'avons montré au cours des 11 années d'existence de ce rapport, le paysage des vulnérabilités Microsoft est en constante évolution. Même si les vulnérabilités représentent une part importante de la surface d'attaque, les investissements dans la recherche et les pratiques de sécurité obligent de plus en plus les auteurs de menaces à innover. Cela continuera de modifier la façon dont les acteurs de menace s'implantent dans les environnements des victimes.



Nous atteignons rapidement un point de basculement où il devient plus facile pour les acteurs malveillants de voler une identité pour y accéder que d'exploiter une vulnérabilité.

Cela signifie que nous pouvons nous attendre à voir le volume et la sophistication des attaques basées sur l'identité augmenter considérablement à mesure que les acteurs de menace se concentrent sur les identités comme moyen d'attaque plus efficace.

Une bonne nouvelle pour les défenseurs est que les principes de sécurité fondamentaux de longue date, éprouvés et testés au cours de la dernière décennie, continuent d'offrir la meilleure ligne de défense, même contre les menaces modernes.

Le moindre privilège est essentiel pour réduire toutes les surfaces d'attaque sur les endpoints et les identités. Moins la victime dispose de privilèges, plus le risque de compromission du compte est faible, même lors d'exploits Zero Day, et même lorsqu'un attaquant procède à l'ingénierie inverse d'un correctif pour trouver une solution de contournement exploitable.

Les organisations qui réussissent à associer les contrôles de sécurité préventifs à la détection et à la réponse aux menaces continueront d'être bien mieux armées pour résister aux menaces de demain. Comme toujours, nous continuerons à proposer nos idées pour aider nos lecteurs à rester attentifs aux dernières menaces, aux vulnérabilités les plus importantes et aux stratégies les plus efficaces pour renforcer leur posture de sécurité.

Méthodologie

Le deuxième mardi de chaque mois (appelé « Patch Tuesday »), Microsoft publie des bulletins de sécurité annonçant les correctifs pour toutes les vulnérabilités affectant les produits Microsoft.

Le rapport annuel BeyondTrust sur les vulnérabilités de Microsoft compile ces versions dans un aperçu sur un an et analyse les données, créant ainsi une vue globale des tendances liées aux vulnérabilités.

Jusqu'en novembre 2020, Microsoft utilisait sa propre méthode de partage des détails CVE via son guide de mise à jour de sécurité.

L'ancien format du rapport Microsoft présentait un résumé pour chaque vulnérabilité signalée qui incluait le verbiage suivant :

- Les clients/utilisateurs dont les comptes sont configurés pour avoir moins de droits utilisateur sur le système pourraient être moins touchés que les utilisateurs qui fonctionnent avec des droits utilisateur administrateur.
- Si l'utilisateur actuel est connecté avec des droits utilisateur administrateur, un attaquant pourrait prendre le contrôle d'un système affecté.

D'après ce résumé, les chercheurs en sécurité pourraient déduire si une vulnérabilité donnée (en particulier les plus critiques) aurait pu être atténuée si les droits administrateur avaient été supprimés.

En 2021, Microsoft a modifié ses méthodologies et est passé à un système commun de notation des vulnérabilités (CVSS). En 2023, Microsoft a continué à utiliser le score CVSS 3.1 pour ses vulnérabilités, mais a commencé à classer les gravités en fonction du propre système d'évaluation de la gravité des mises à jour de sécurité de Microsoft.

La méthodologie CVSS permet de croiser plus facilement les vulnérabilités Microsoft avec des bugs tiers, simplifiant ainsi certaines analyses. Le système d'évaluation de la gravité des mises à jour de sécurité de Microsoft permet d'évaluer chaque vulnérabilité en fonction du pire résultat théorique, si cette vulnérabilité était exploitée.

Cependant, un compromis malheureux de ce changement a été la perte de la capacité à déterminer l'impact des droits administrateur sur les vulnérabilités critiques.

Non seulement les risques d'accès privilégiés excessifs restent tout à fait intacts, mais les vecteurs d'attaque privilégiés se développent rapidement avec l'expansion du cloud et la prolifération des identités et des comptes humains et machines.

Ainsi, même si les statistiques sur les droits administrateur sont absentes du rapport de cette année, il est impératif que les organisations ne fassent pas preuve de complaisance. La suppression des droits administrateur reste un élément clé d'une stratégie de moindre privilège, ainsi que pour permettre le Zero Trust.

Exactitude des données de vulnérabilité

Un certain nombre de généralisations ont été faites pour chaque vulnérabilité, telles que :

- Chaque vulnérabilité a été classée avec un indice de gravité le plus élevé de toutes les instances de cette vulnérabilité où elle est apparue plusieurs fois.
- Chaque vulnérabilité a été classée selon le type le plus répandu pour toutes les instances de cette vulnérabilité
- Les versions de produits n'ont pas été prises en compte.
- Les combinaisons de produits n'ont pas été prises en compte.
- Les vulnérabilités ont été prises en compte 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 pour Microsoft. Edge et Windows).

>>> Ressources additionnelles

ÉVALUATION	**Prenez le contrôle sur l'ensemble de votre surface d'attaques d'identité.** Commencez par une évaluation gratuite de la sécurité des identités et une surveillance de votre parc IT pour mettre en évidence les privilèges excessifs, les mauvaises configurations (manque de MFA, etc., comptes orphelins, attaques en cours et bien plus). Obtenez également des informations claires sur le contexte des menaces et les mesures correctives.
TEST/LISTE DE CONTRÔLE	**Besoin d'une alternative VPN ?** Faites le test d'accès à distance : découvrez si votre équipe dispose des outils d'accès à distance sécurisés appropriés pour gérer un grand nombre d'utilisateurs qui se connectent à distance à votre réseau.
LISTE DE CONTRÔLE	**Liste de contrôle pour la cyber assurance :** Utilisez notre liste de contrôle pour déterminer dans quelle mesure votre organisation répond aux exigences strictes nécessaires pour être cyber assuré.
GUIDE DE SOLUTIONS	**Un guide sur Endpoint Privilege Management :** Découvrez comment la gestion des endpoints privilégiés (EPM) combine le moindre privilège avec le contrôle des applications pour réduire considérablement la surface d'attaque sur Windows, macOS et Linux.
LIVRE BLANC	**Guide de l'acheteur pour une gestion complète des accès à privilèges (PAM) :** Comprenez les fonctionnalités PAM indispensables nécessaires pour sécuriser correctement les identités et les accès dans votre environnement, éliminer et atténuer de nombreux vecteurs de menaces et vous aider à avancer dans votre parcours PAM.
BLOG	**Abri. from the Storm – Ce que l'attaque de Midnight Blizzard contre Microsoft nous apprend sur les attaques modernes basées sur l'identité :** Découvrez les caractéristiques uniques qui distinguent cette attaque et découvrez pourquoi cette attaque d'un État-nation contre Microsoft souligne l'importance d'une approche de la sécurité axée sur l'identité.

À propos de BeyondTrust

BeyondTrust est le leader mondial de la gestion intelligente des identités et de la sécurisation des accès, permettant aux organisations de protéger les identités, de contrer les menaces et de fournir un accès dynamique. Nous offrons la seule plateforme dotée à la fois d'une détection intelligente des menaces liées à l'identité et d'un contrôle des privilèges. Nos solutions garantissent un Zero Trust basées sur le principe du moindre privilège afin de réduire votre surface d'attaque et d'éliminer les angles morts en matière de sécurité.

BeyondTrust protège les identités, les accès et les endpoints dans l'ensemble de votre organisation, tout en créant une expérience utilisateur de qualité et une grande efficacité opérationnelle. Nous sommes à la pointe de l'innovation en matière de sécurisation des identités et bénéficions de la confiance de 20 000 clients, dont 75 font partie du classement Fortune 100, ainsi que d'un écosystème mondial de partenaires.
Pour en savoir plus, rendez-vous sur **www.beyondtrust.com/fr.**