



CISA révèle le **top 30** des **vulnérabilités** les plus exploitées depuis **2020**






Accrochez-vous, les amis! Les fédéraux ont lâché le top 30 des vulnérabilités activement utilisées par les hackers depuis 2020. Un récent avis conjoint publié par l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) - conjointement avec le Centre australien de cybersécurité (ACSC), le Centre national de cybersécurité (NCSC) du Royaume-Uni et le Bureau fédéral d'enquête (FBI) des États-Unis - détaille les vulnérabilités qui ont été couramment exploitées en 2020 et 2021.

Qu'attendez-vous pour agir? Commencez à analyser votre réseau à la recherche des CVE mentionnées ci-dessous et assurez-vous d'avoir des correctifs pour éviter de rejoindre le club très peuplé des victimes de la cybercriminalité. Le CISA révèle le top 30 des vulnérabilités les plus exploitées depuis 2020.

Vulnérabilités célèbres couramment exploitées en 2020

PRODUITS AFFECTÉS	CVE	CVSS	IMPACT
 Citrix Application Delivery Controller (ADC) et Citrix Gateway	CVE-2019-19781	9.8	Traversée de répertoire
 Pulse Connect Secure	CVE-2019-11510	10	Lecture de fichiers arbitraires
 Fortinet FortiOS	CVE-2018-13379	9.8	Faible de traversée de chemin menant à une fuite de fichier système
 F5 BIG-IP	CVE-2020-5902	9.8	Exécution de code à distance
 MobileIron Core & Connector	CVE-2020-15505	9.8	Exécution de code à distance
 Microsoft Exchange Server	CVE-2020-0688	8.8	Corruption de mémoire
 Atlassian Confluence Server	CVE-2019-3396	9.8	Exécution de code à distance
 Microsoft Office	CVE-2020-15505	7.8	Corruption de mémoire
 Atlassian Crowd et Crowd Data Center	CVE-2019-11580	9.8	Exécution de code à distance
 Drupal	CVE-2018-7600	9.8	Exécution de code à distance
 Telerik UI pour ASP.NET AJAX	CVE-2019-18935	9.8	Exécution de code à distance
 Microsoft SharePoint	CVE-2019-0604	9.8	Exécution de code à distance
 Windows Background Intelligent	CVE-2020-0787	7.8	Élévation de privilège
 Windows Netlogon	CVE-2020-1472	10	Élévation de privilège

Qu'est-ce qui a attiré l'attention des hackers en 2021?

PRODUITS AFFECTÉS	CVE	CVSS	IMPACT
 <p>Pulse Secure Pulse Connect Secure</p>	CVE-2021-22893	10	Exécution de code arbitraire à distance
	CVE-2021-22894	8.8	Exécution de code arbitraire à distance
	CVE-2021-22899	8.8	Exécution de code à distance
	CVE-2021-22900	7.2	Injection de code
 <p>Exchange Microsoft Exchange Server</p>	CVE-2021-26855	9.8	Exécution de code à distance
	CVE-2021-26857	7.8	Exécution de code à distance
	CVE-2021-26858	7.8	Exécution de code à distance
	CVE-2021-27065	7.8	Exécution de code à distance
 <p>Accellion</p>	CVE-2021-27101	9.8	Injection SQL
	CVE-2021-27102	7.2	Injection de commande OS
	CVE-2021-27103	9.8	Falsification de requête côté serveur (SSRF)
	CVE-2021-27104	9.8	Exécution de commandes du système d'exploitation
 <p>vmware® VMware</p>	CVE-2021-21985	9.8	Exécution de code à distance
 <p>FORTINET Fortinet</p>	CVE-2018-13379	9.8	Traversée de chemin
	CVE-2020-12812	9.8	Authentification incorrecte
	CVE-2019-5591	6.5	Configuration vulnérabilité

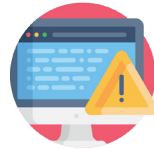
Que pouvons-nous apprendre de ces exploitations?



Les attaques de type "zero day" sont rares. Les attaquants sont plus susceptibles d'exploiter les vulnérabilités connues de produits importants, car cela leur permet d'utiliser les failles comme armes contre de vastes ensembles de cibles dans le monde entier. Il est surprenant de constater que les vulnérabilités datant de plusieurs années peuvent encore être exploitées, comme le prouve l'exploitation en cours de CVE-2017-11882, qui date de plusieurs années. C'est également un indicateur de la fréquence à laquelle de nombreuses organisations continuent d'utiliser les produits concernés sans correction.



L'expansion sans précédent du travail à distance explique l'exploitation accrue des vulnérabilités en 2020 et 2021. Le changement rapide de paradigme a compliqué la tâche des équipes de sécurité, qui ne pouvaient pas suivre le rythme des correctifs de routine sur les machines distantes.



Les attaques de type "zero day" sont rares. Les attaquants sont plus susceptibles d'exploiter les vulnérabilités connues de produits importants, car cela leur permet d'utiliser les failles comme armes contre de vastes ensembles de cibles dans le monde entier.



Quatre des vulnérabilités les plus ciblées existent dans les passerelles VPN et d'autres outils qui offrent un accès à distance.

Comment garder les vulnérabilités à distance

Le CISA recommande vivement aux organisations de mettre en place un système centralisé de gestion des correctifs et de donner la priorité aux correctifs des vulnérabilités les plus exploitées. Si vous cherchez le bon outil, ne cherchez pas plus loin. ManageEngine vous propose trois solutions qui peuvent faire des correctifs un jeu d'enfant. Qu'il s'agisse de rechercher en permanence les failles de sécurité sur vos terminaux distribués, de tester et de déployer les correctifs, tout peut être automatisé à partir d'un seul et même écran.

Endpoint Central

Endpoint Central est une solution unifiée de gestion et de sécurité des terminaux qui couvre l'ensemble du cycle de vie de la gestion des terminaux, notamment l'automatisation des correctifs, le déploiement de logiciels, la prise de contrôle des postes de travail distants, la gestion et la supervision des actifs, des licences logicielles, de l'utilisation des logiciels et des périphériques USB, et bien plus encore.

ESSAI GRATUIT

Vulnerability Manager Plus

Vulnerability Manager Plus est un outil de gestion des menaces et des vulnérabilités axé sur la hiérarchisation, destiné aux entreprises et offrant une gestion intégrée des correctifs.

ESSAI GRATUIT

Patch Manager Plus

Patch Manager Plus est une solution complète de gestion des correctifs offrant un déploiement automatisé des correctifs pour les terminaux Windows, macOS et Linux ainsi que pour plus de 500 applications tierces.

ESSAI GRATUIT