AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

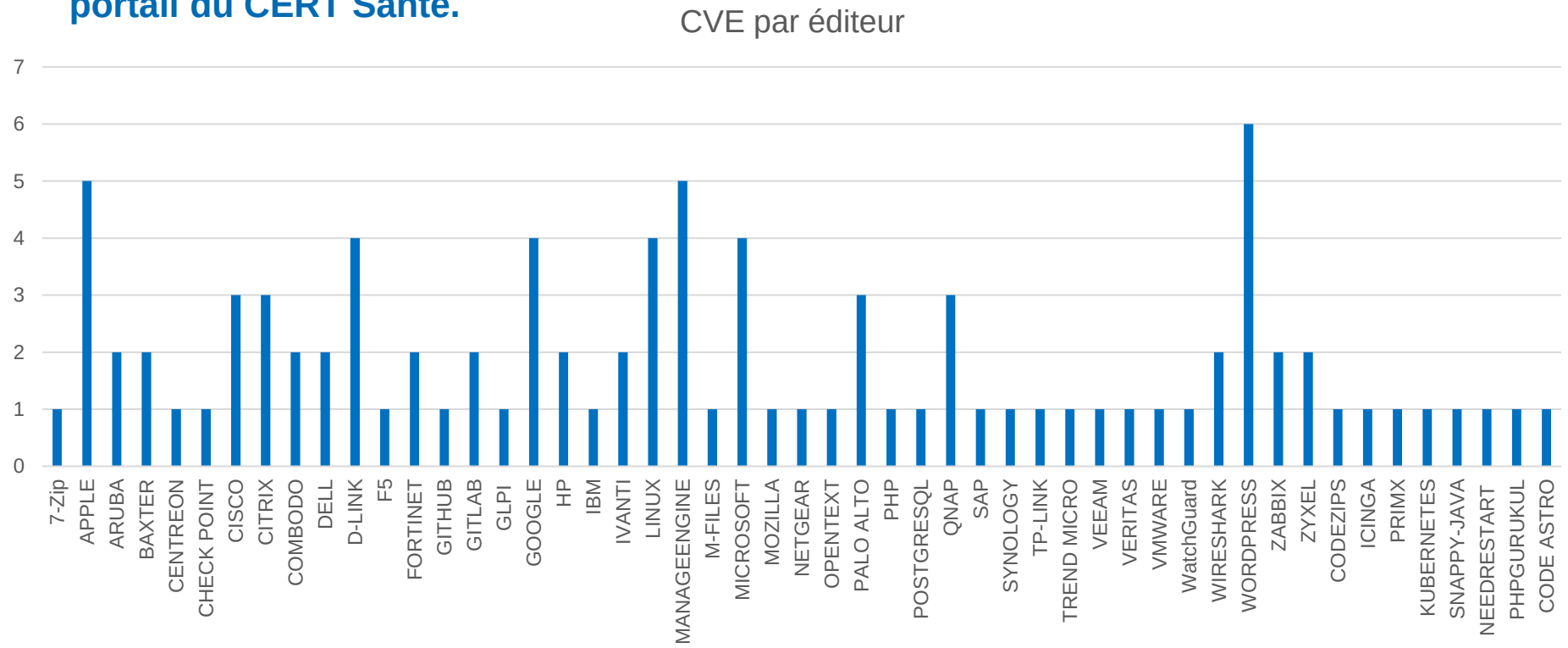
Indicateurs sur la publication des CVE pour le mois de novembre 2024

CERT Santé

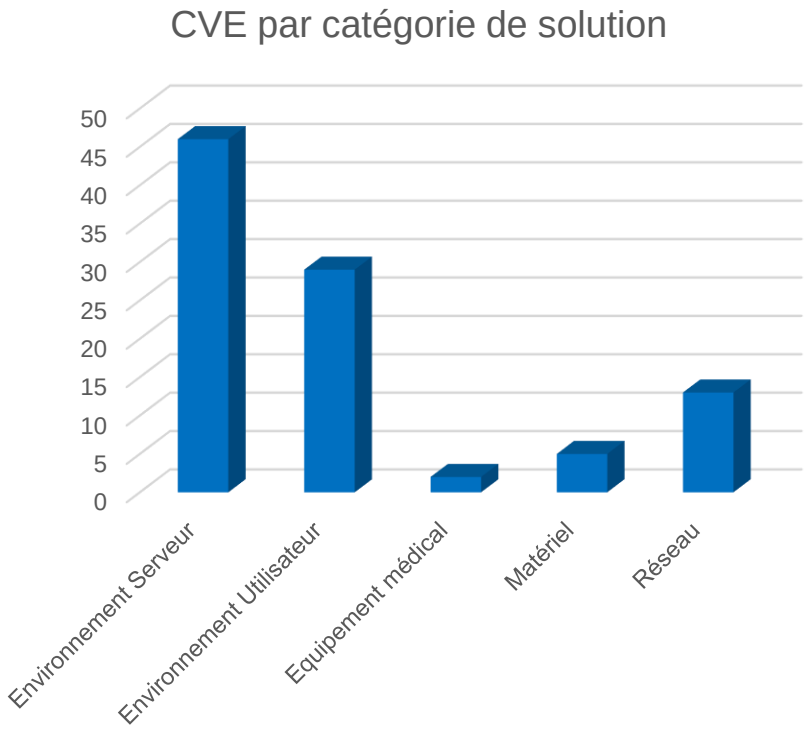
Décembre 2024

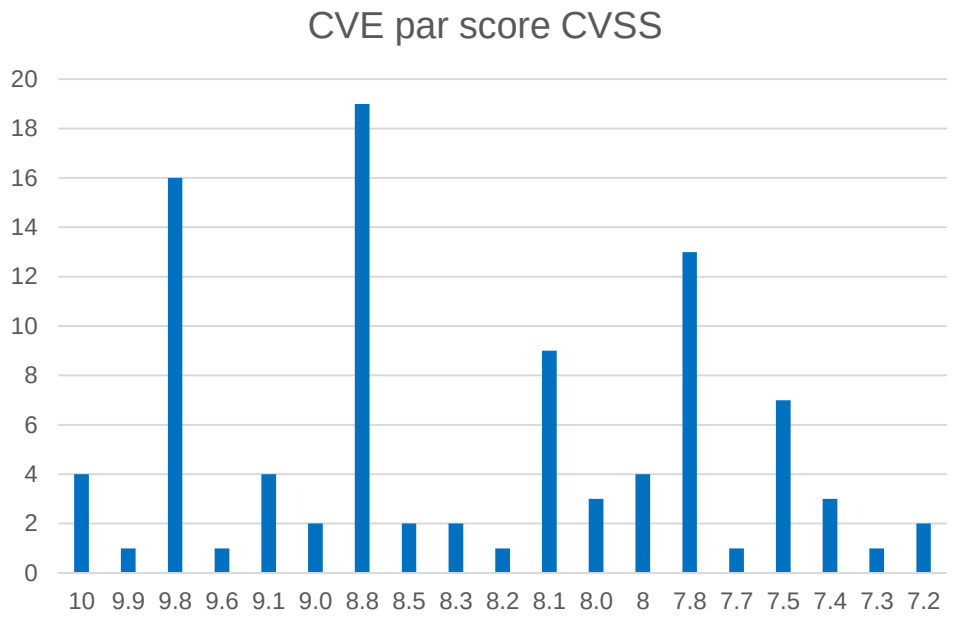
Nombre de CVE par éditeur

95 vulnérabilités ont été analysées et publiées (parmi lesquelles 9 alertes) sur le portail du CERT Santé.



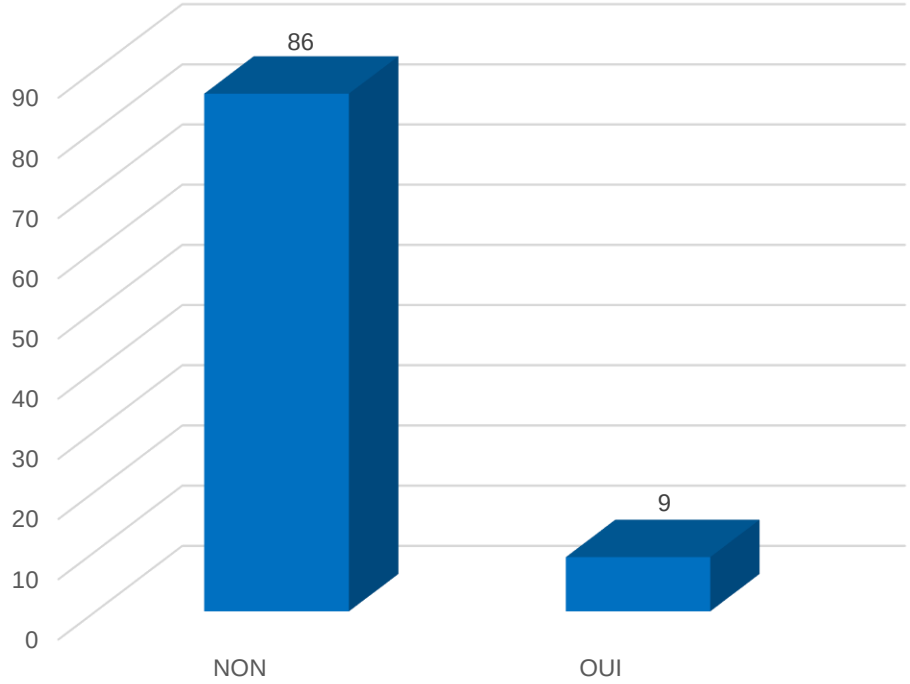
Nombre de CVE par catégorie de produit et score CVSS



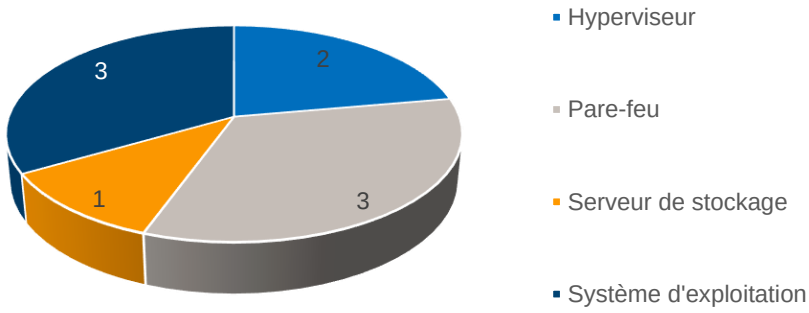


Vulnérabilités exploitées

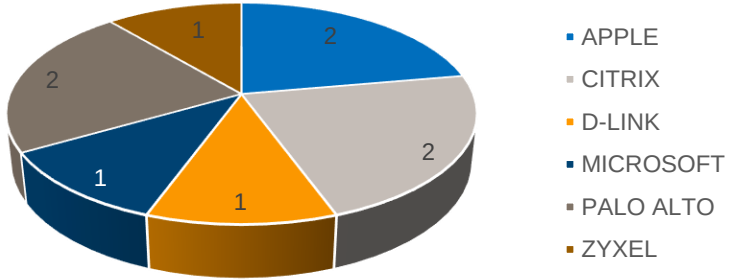
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

9.8

Palo Alto

Contournement de la politique de sécurité

Exploitée

(CVE-2024-0012)

Un défaut dans Palo Alto Networks permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'obtenir les privilèges administrateur, de modifier les configurations ou d'exploiter d'autres vulnérabilités de type élévation de privilèges comme la CVE-2024-9474.

Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

8.8

Microsoft

Contournement de la politique de sécurité

Exploitée

(CVE-2024-49039)

Un défaut dans le planificateur de tâches de Microsoft permet à un attaquant authentifié, en exécutant une application spécifiquement forgée, de s'échapper de la Sandbox et d'exécuter des fonctions RPC disponibles seulement à des comptes privilégiés.

Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

7.5

Zyxel

Exécution de code arbitraire

Exploitée

(CVE-2024-11667)

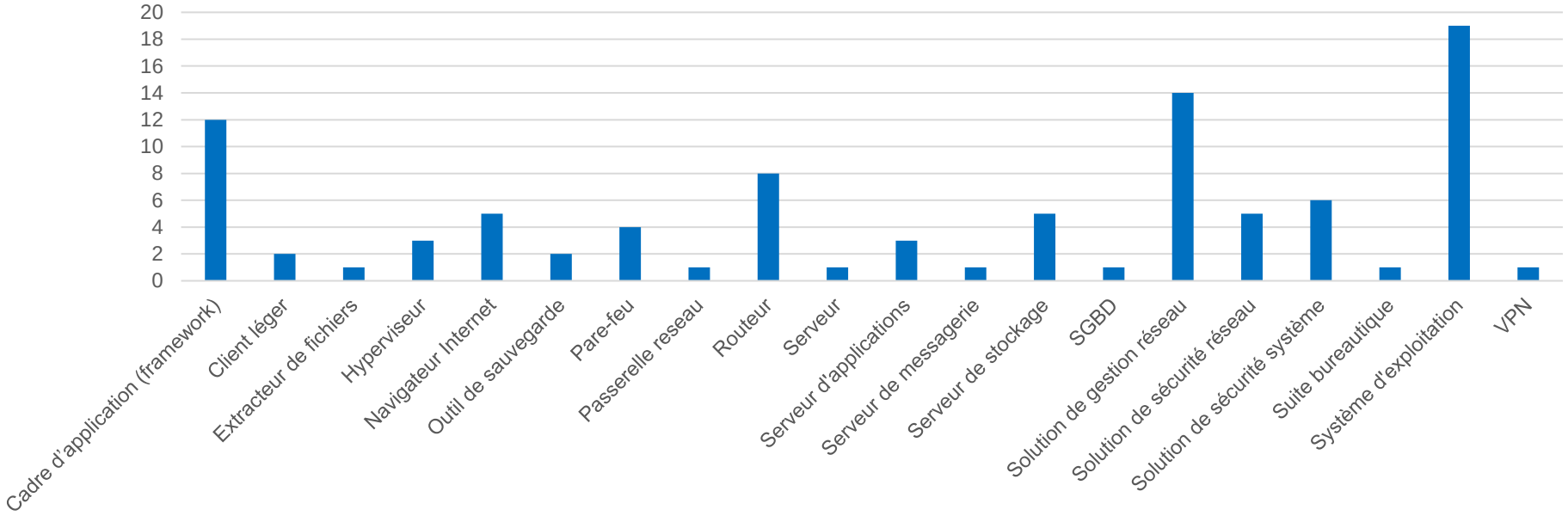
Une vulnérabilité de type traversée de chemins dans l'interface Web des pare-feux Zyxel ZLD permet à un attaquant non authentifié, en envoyant des requêtes *via* une URL spécifiquement forgée, de télécharger ou de téléverser des fichiers.

Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

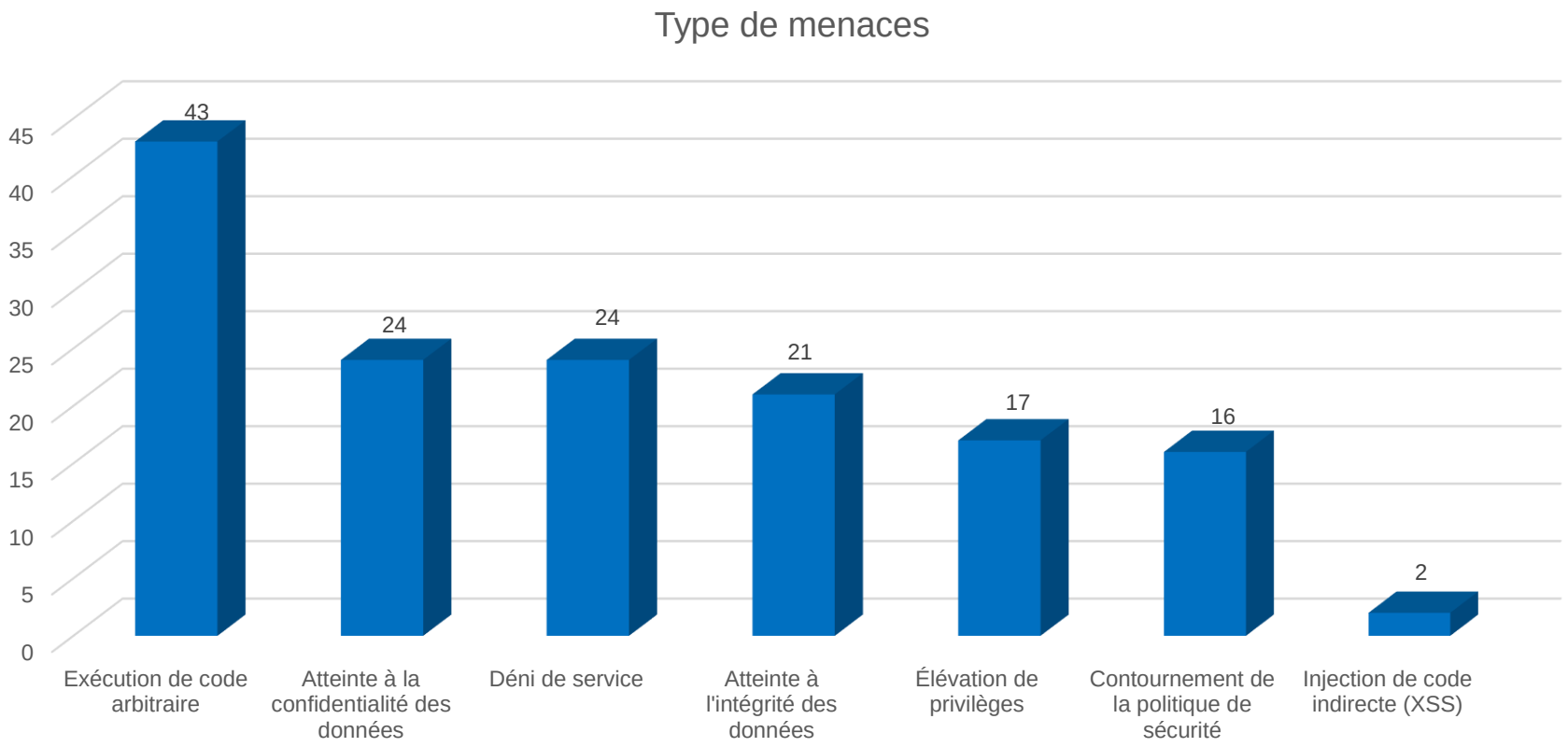
Types de solutions vulnérables

Les systèmes d'exploitation, les solutions de gestion réseau et les cadres d'application sont les principaux types d'équipements affectés par les vulnérabilités publiées.

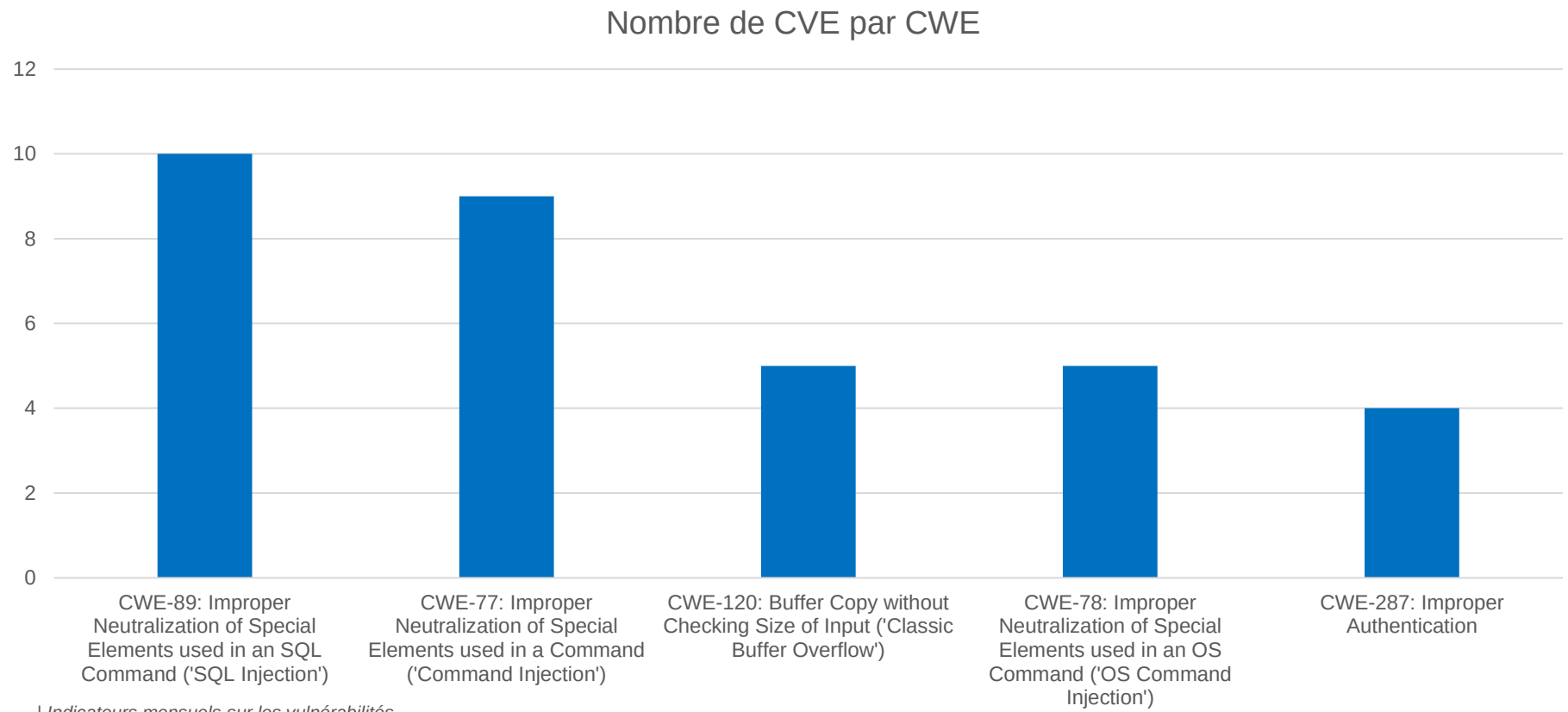
CVE par type de solution



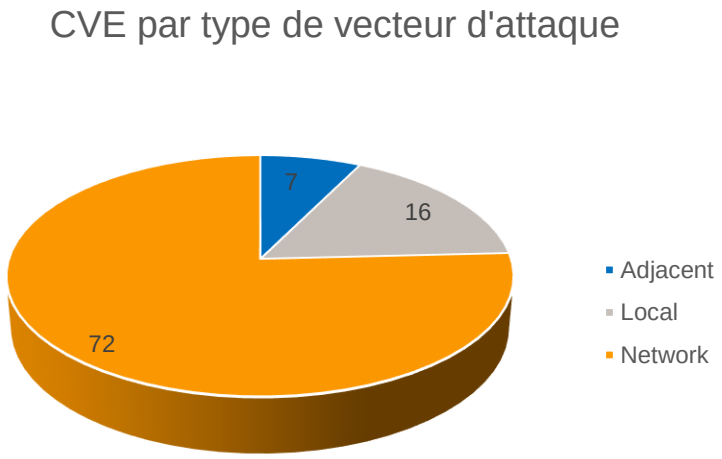
Types de menaces

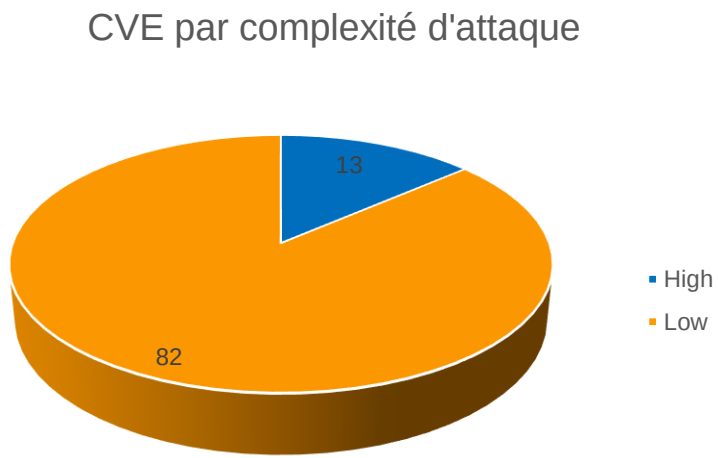


TOP 6 des failles selon le référentiel CWE



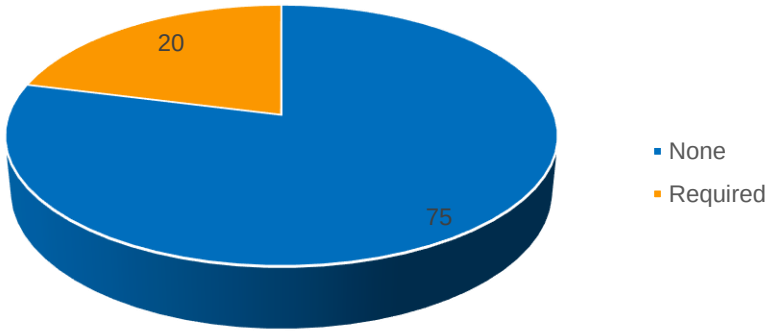
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



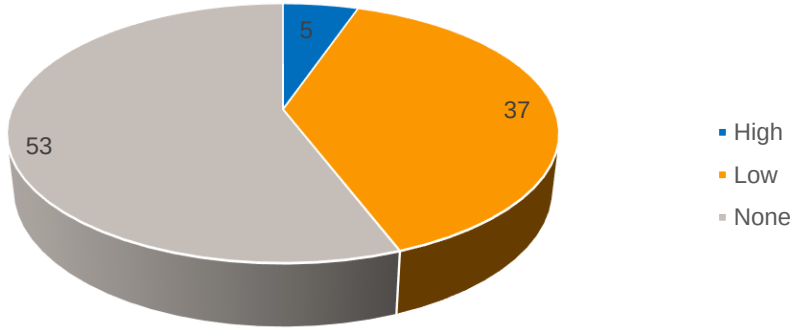


Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

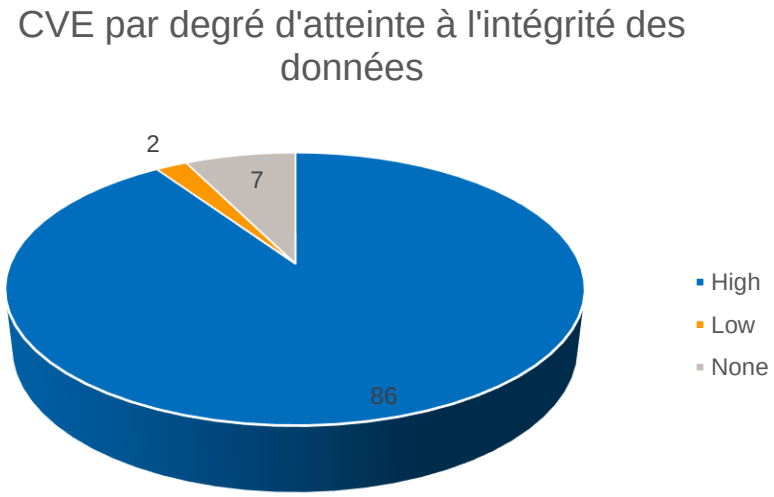
CVE par interaction utilisateur

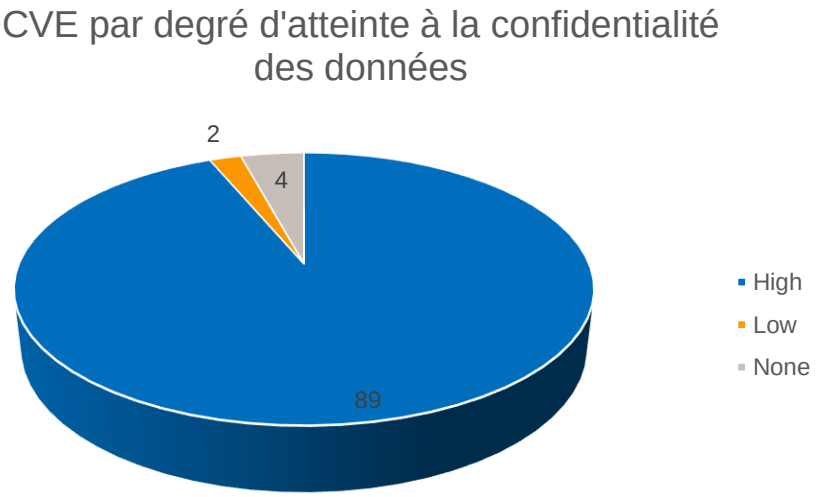


CVE par type de privilèges requis

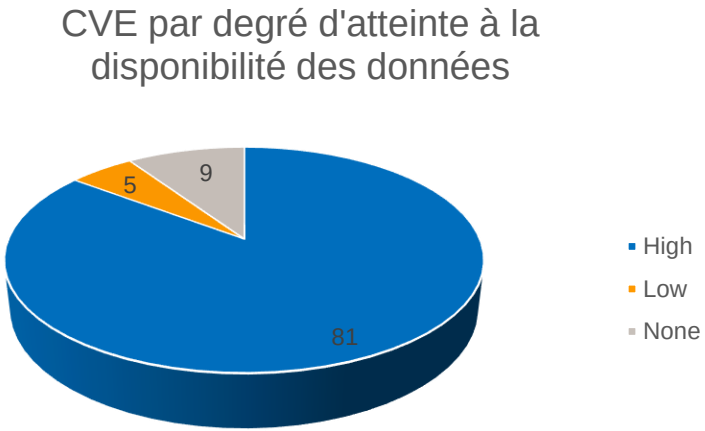


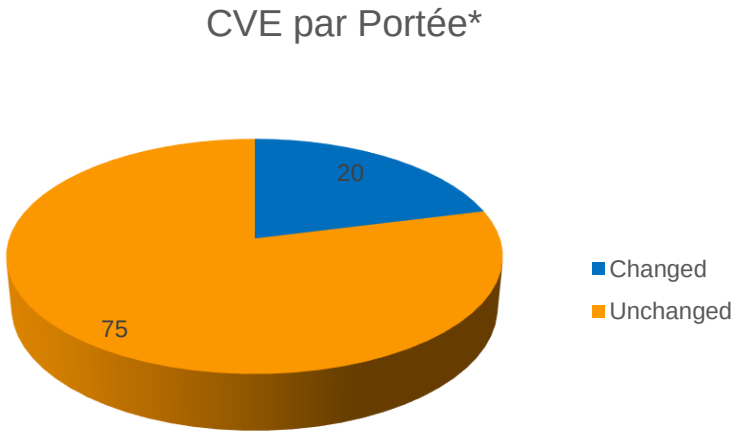
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données





Nombre de CVE selon l'impact sur la disponibilité des données et la portée





*La portée dans un score CVSS confirme ou infirme le fait que la vulnérabilité d'un composant a un impact sur les ressources d'autres composants situés au-delà du périmètre de sécurité géré par l'autorité de sécurité du composant vulnérable.