AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

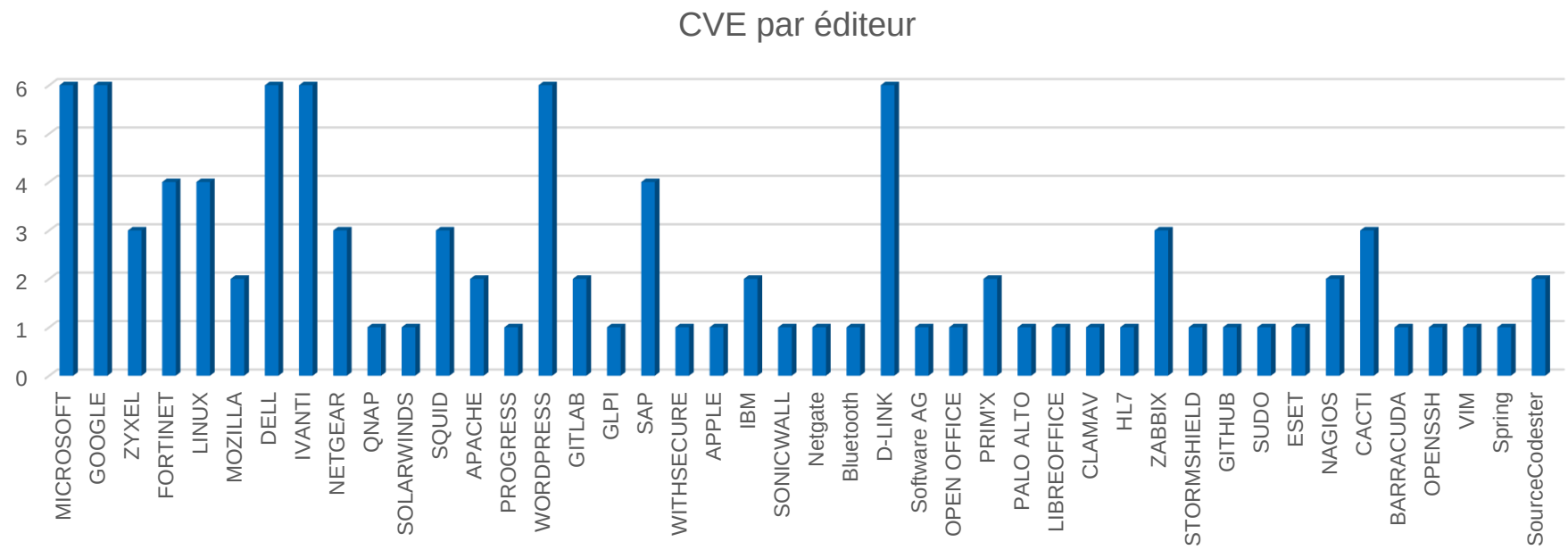
Indicateurs sur la publication des CVE pour le mois de décembre 2023

CERT Santé

Janvier 2024

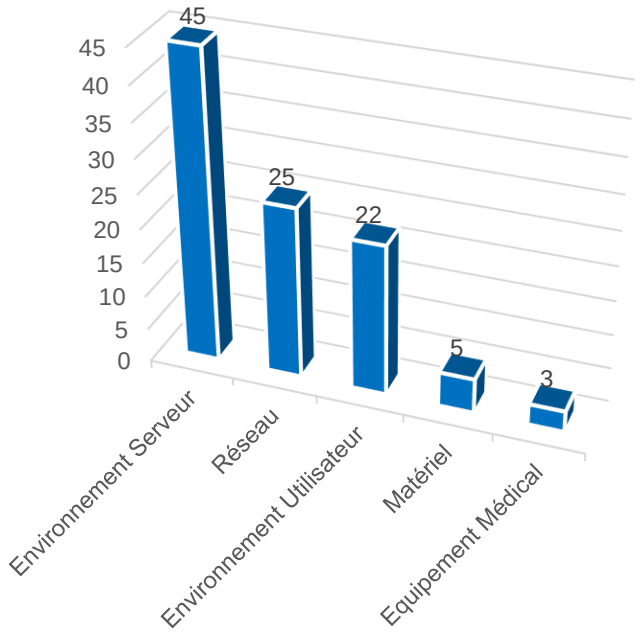
Nombre de CVE par éditeur

100 vulnérabilités ont été analysées et publiées (parmi lesquelles 6 alertes) sur le portail du CERT Santé.

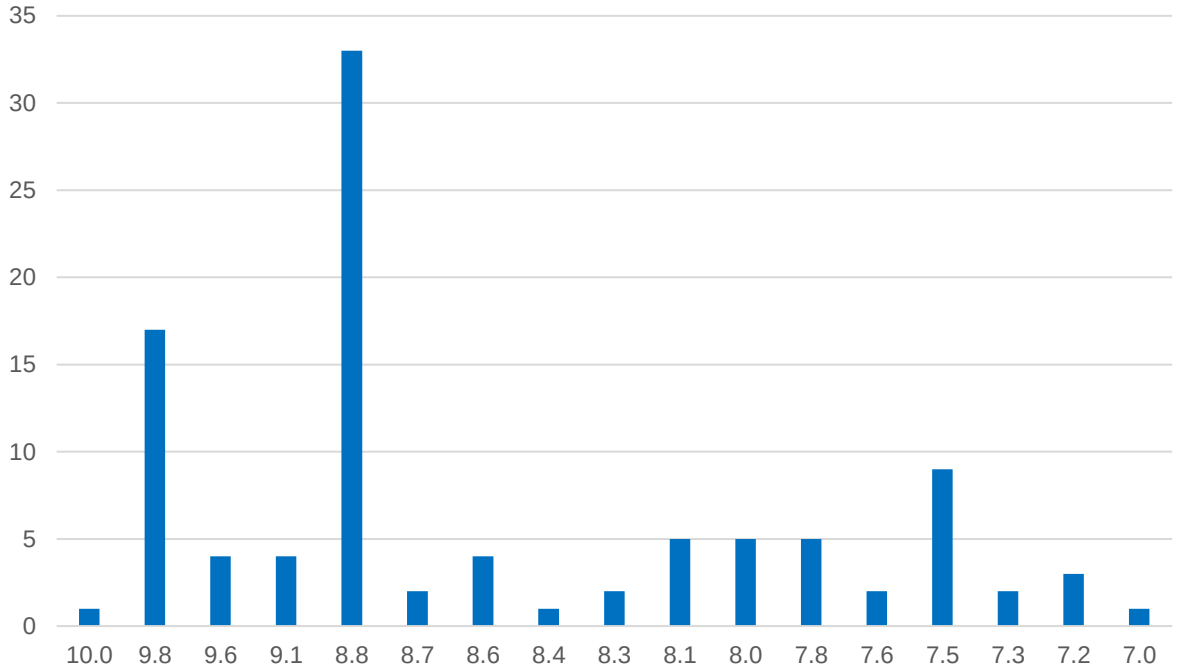


Nombre de CVE par catégorie de produit et score CVSS

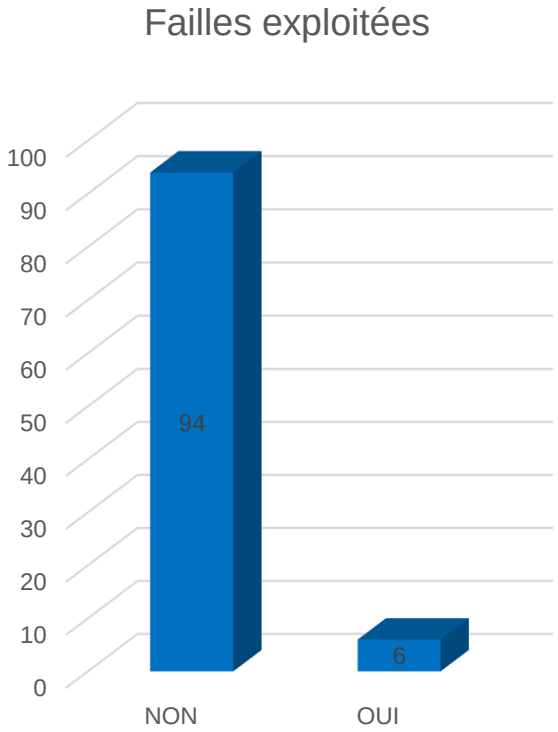
CVE par catégorie de solution

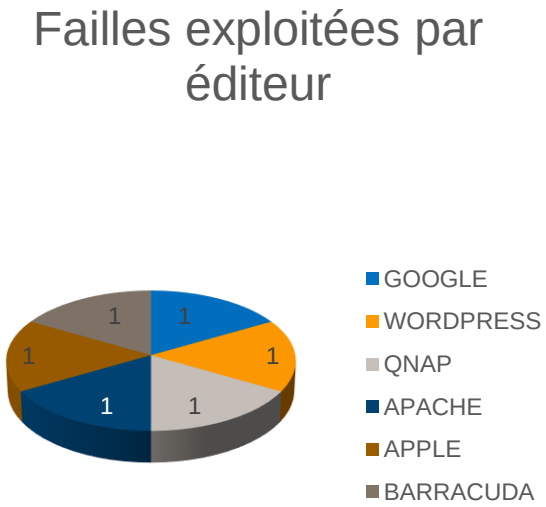


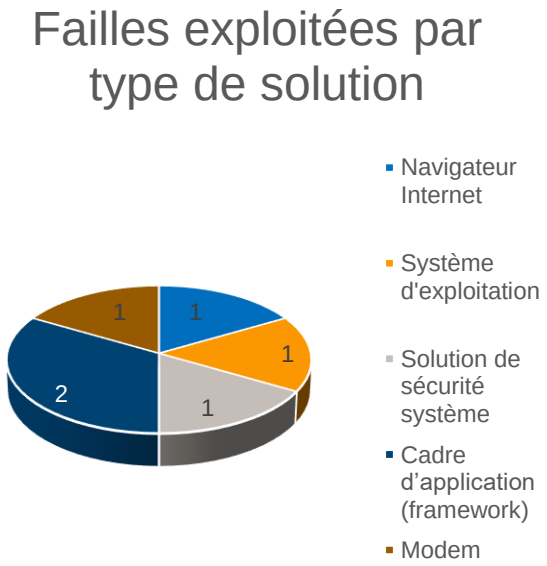
CVE par score CVSS



Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

9.8

Apache Struts
(CVE-2023-50164)

Exécution de code arbitraire

Exploitée

Un attaquant distant et non authentifié peut exécuter du code arbitraire sur le système via une faille de type traversée de répertoires.

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

8.8

Google Chrome
(CVE-2023-7024)

Exécution de code arbitraire

Exploitée

Un attaquant non authentifié peut exécuter du code arbitraire, en persuadant une victime de consulter un site forgé.

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

8

QNAP
(CVE-2023-47565)

Exécution de code arbitraire

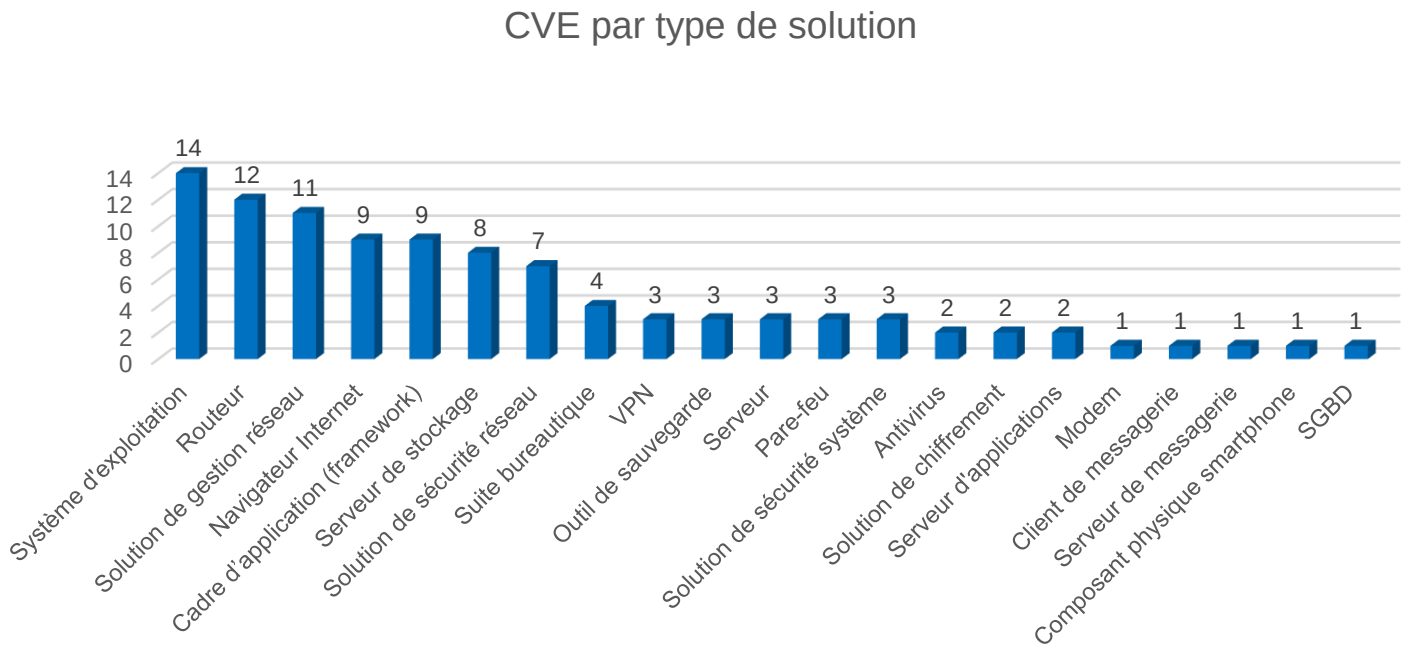
Exploitée

Un attaquant authentifié peut exécuter du code arbitraire via une faille de type injection de commandes.

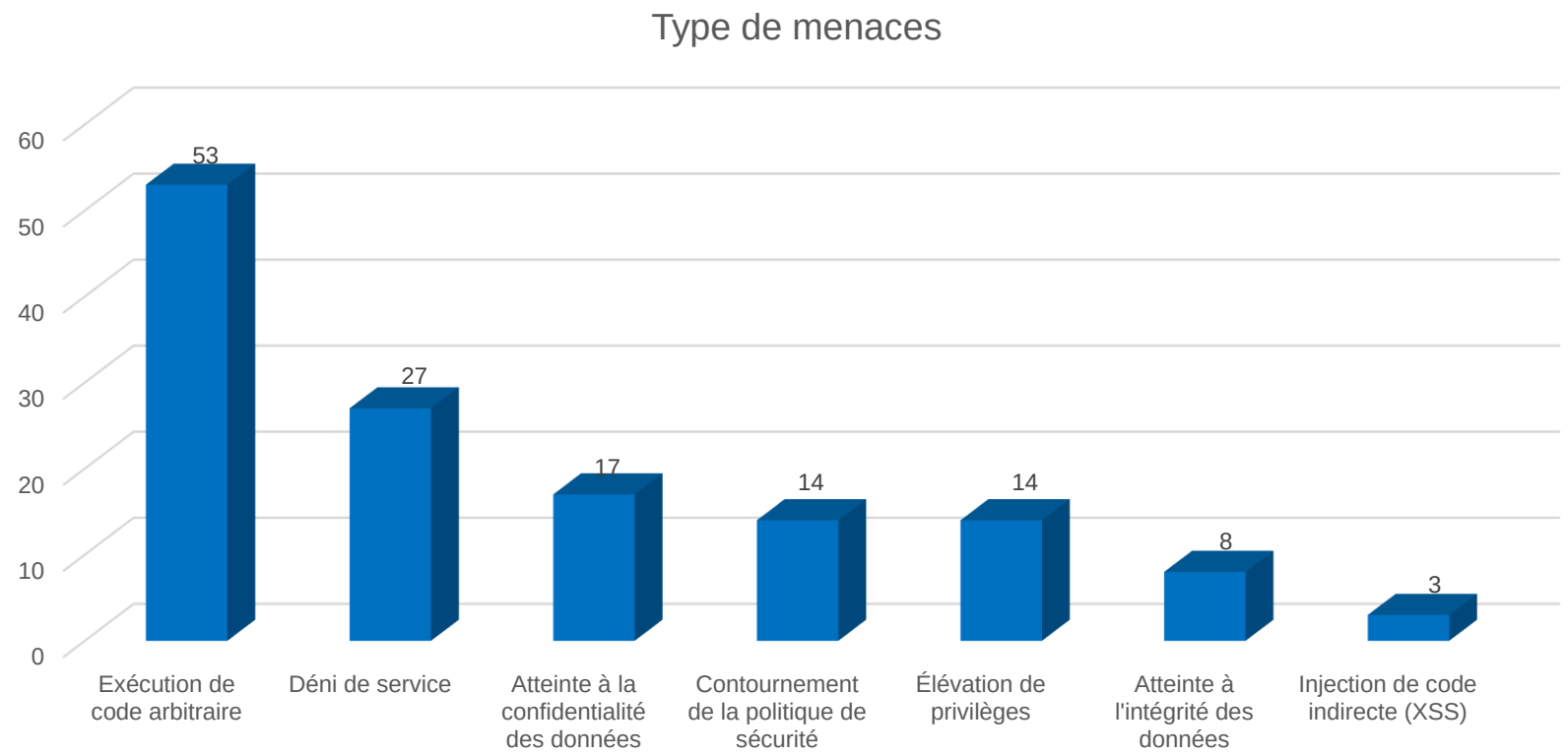
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solution vulnérables

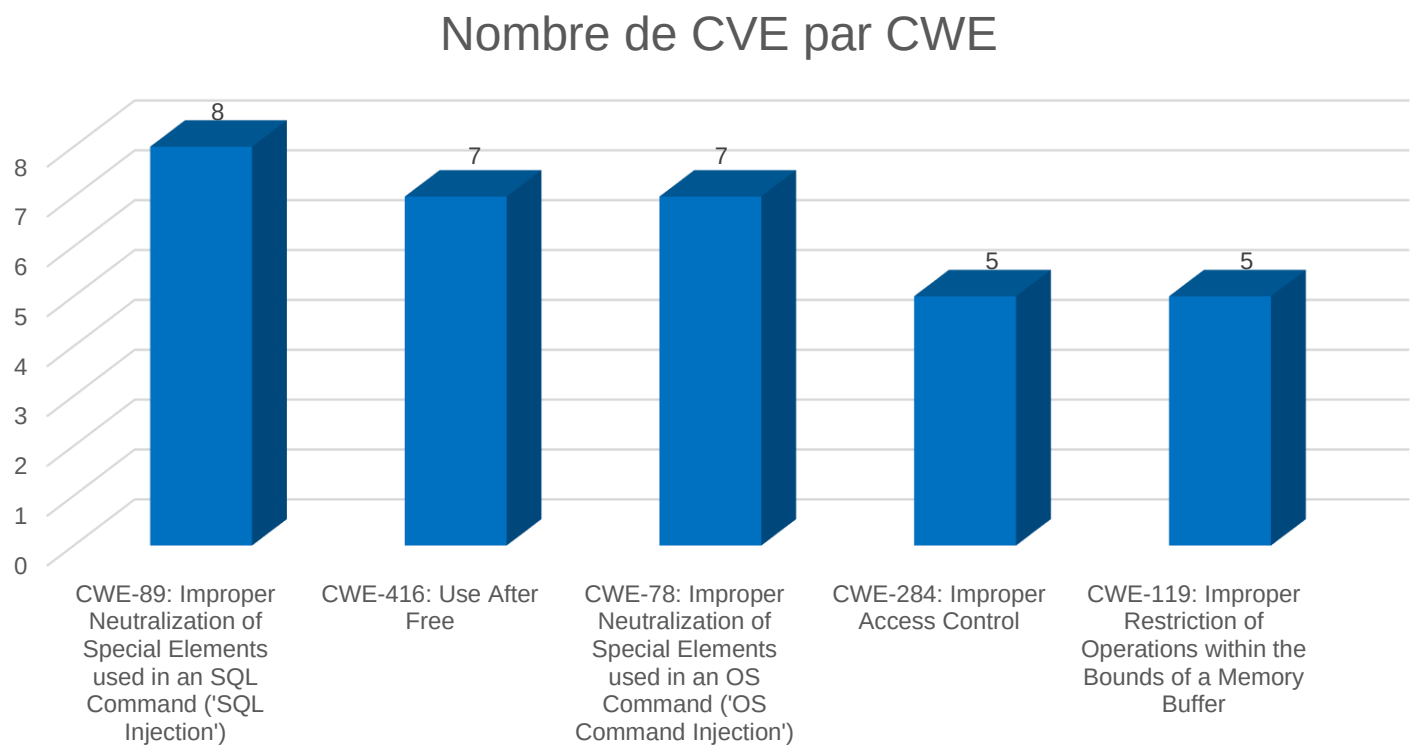
Les systèmes d'exploitation, les routeurs et les solutions de gestion réseau sont les principaux types d'équipements affectés par les vulnérabilités publiées.



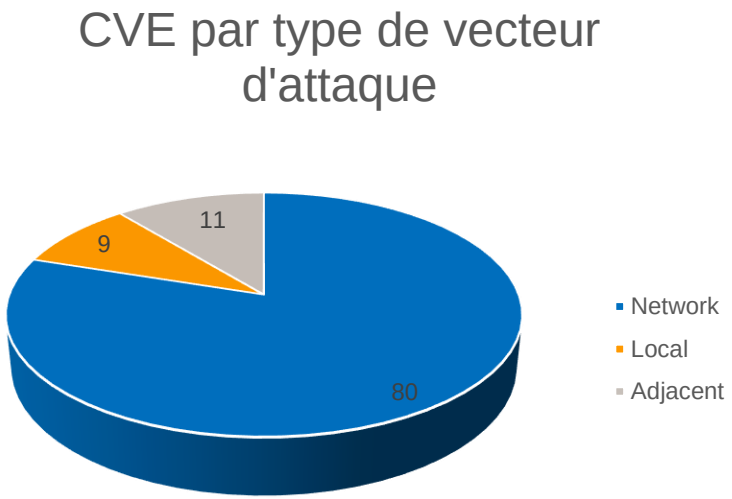
Types de menaces

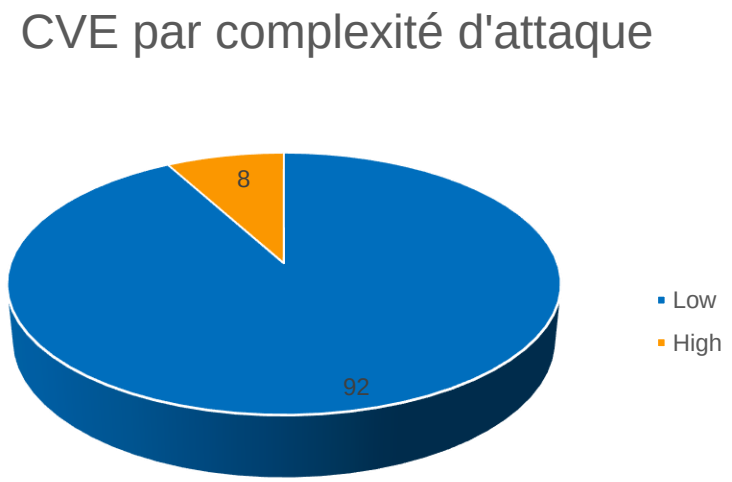


TOP 5 des failles selon le référentiel CWE



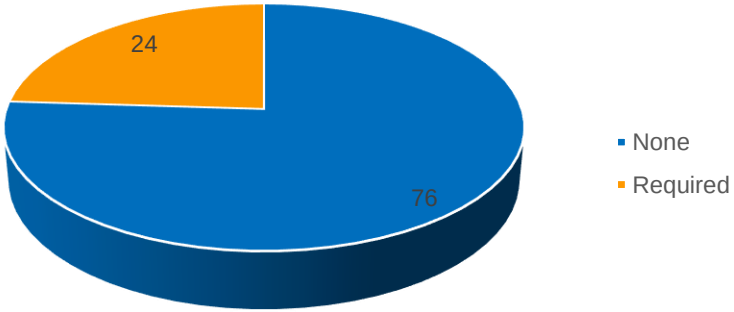
Nombre de CVE selon le vecteur d’attaque et la complexité de l’attaque



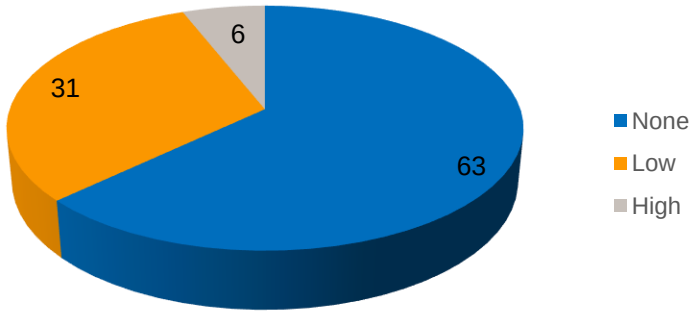


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

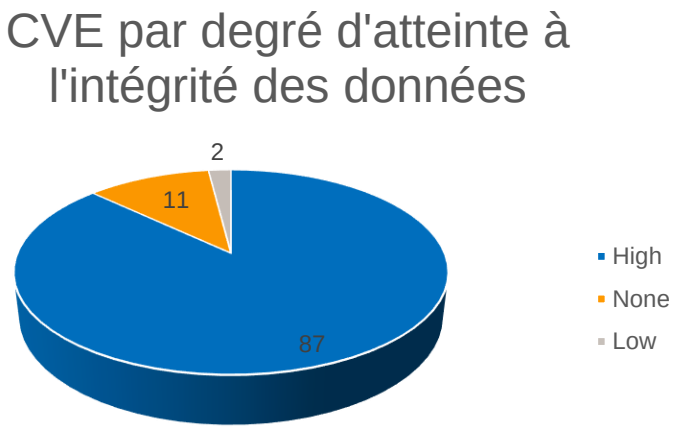
CVE par interaction utilisateur

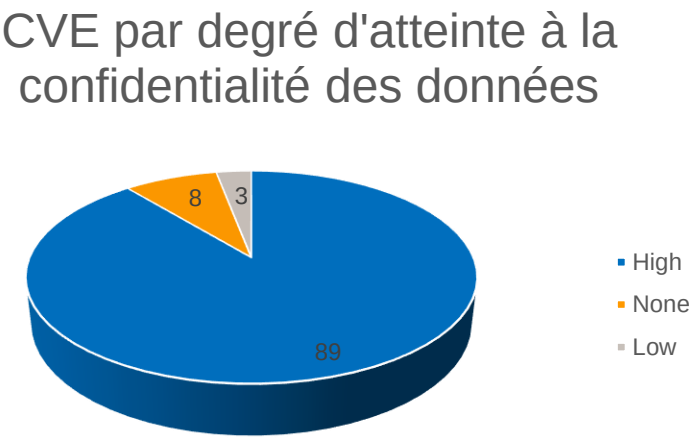


CVE par type de privilège requis

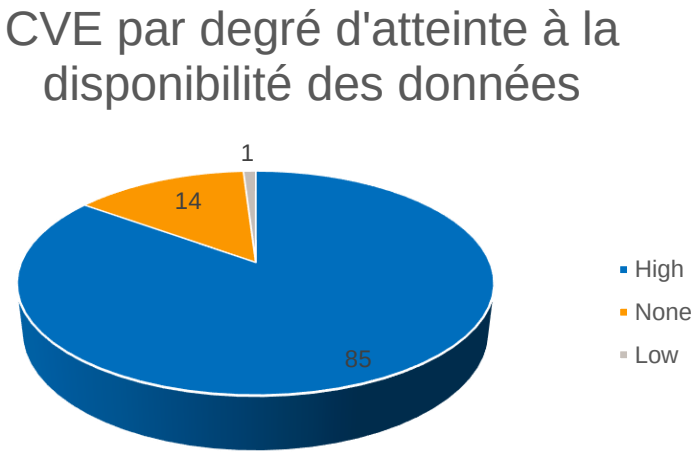


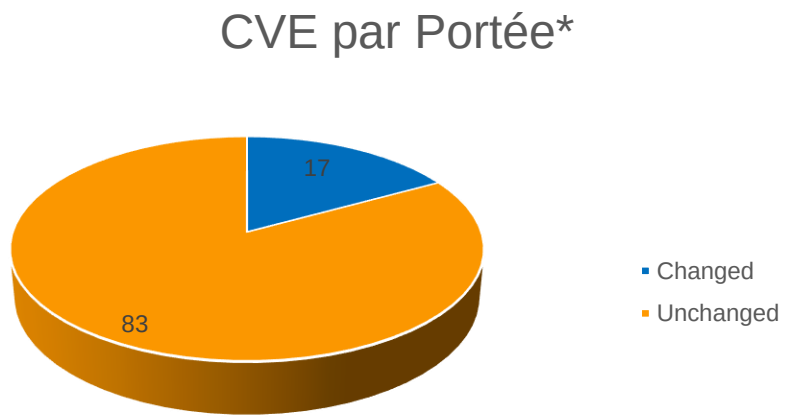
Nombre de CVE selon l’impact sur l’intégrité et sur la confidentialité des données





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.