AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

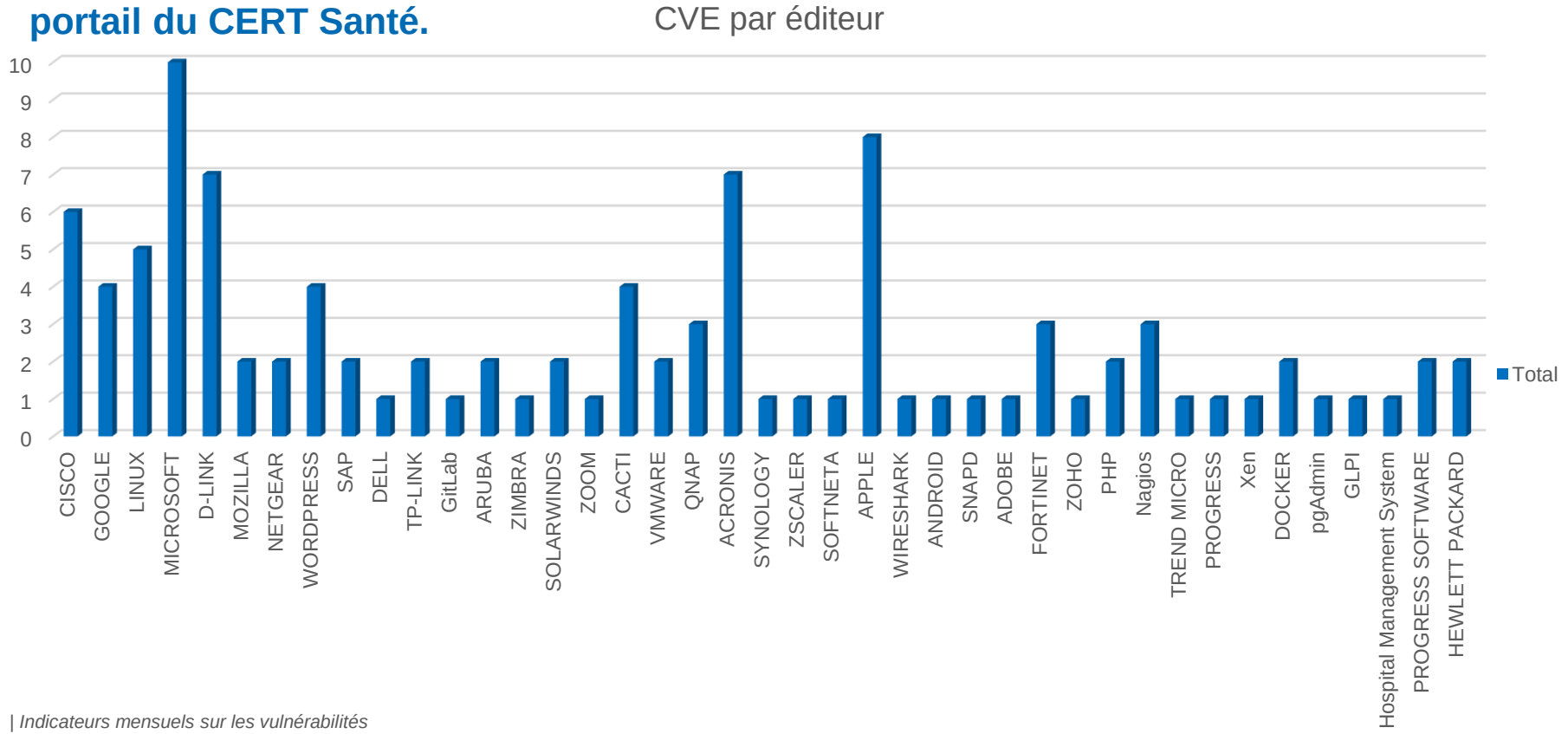
Indicateurs sur la publication des CVE pour le mois de septembre 2023

CERT Santé

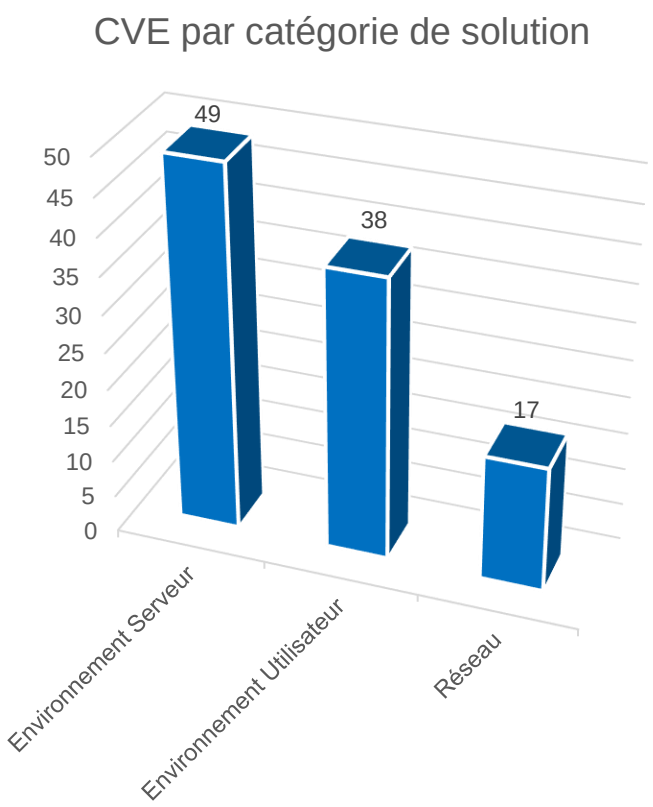
Octobre 2023

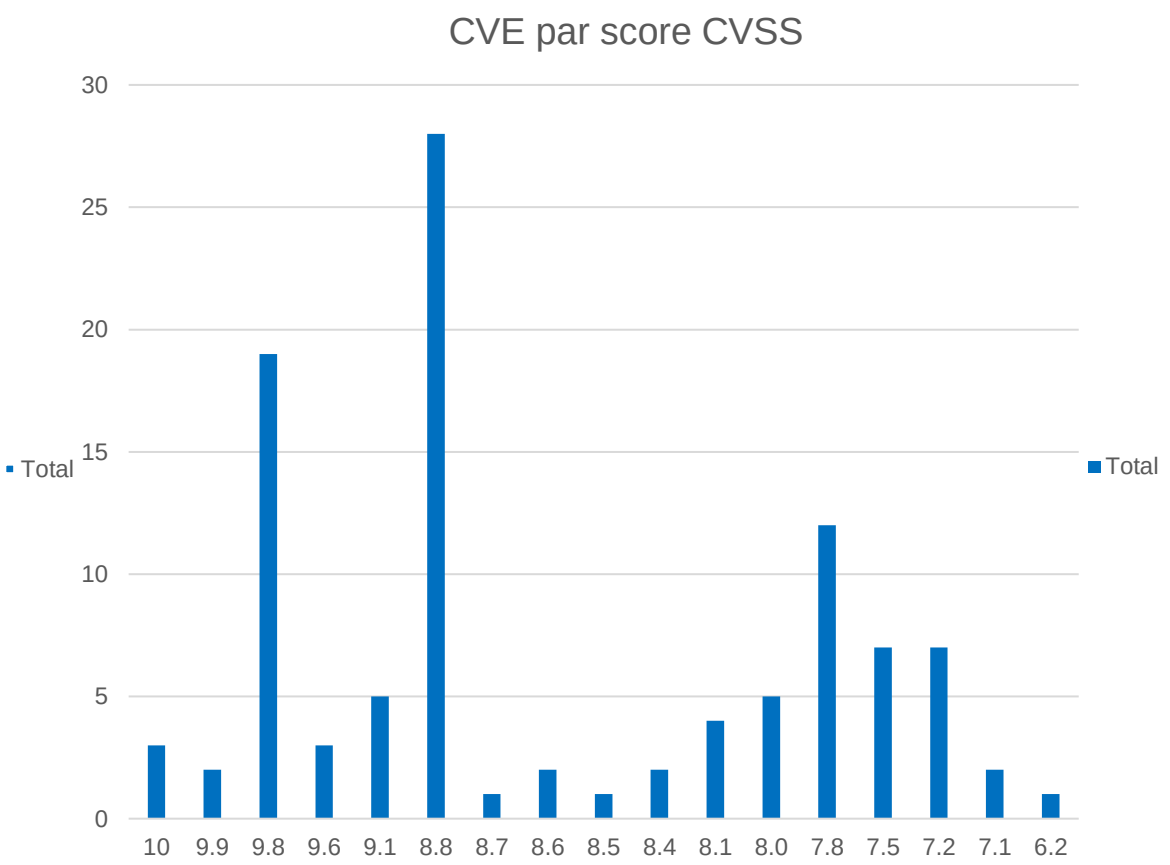
Nombre de CVE par éditeur

104 vulnérabilités ont été analysées et publiées (parmi lesquelles 16 alertes) sur le portail du CERT Santé.



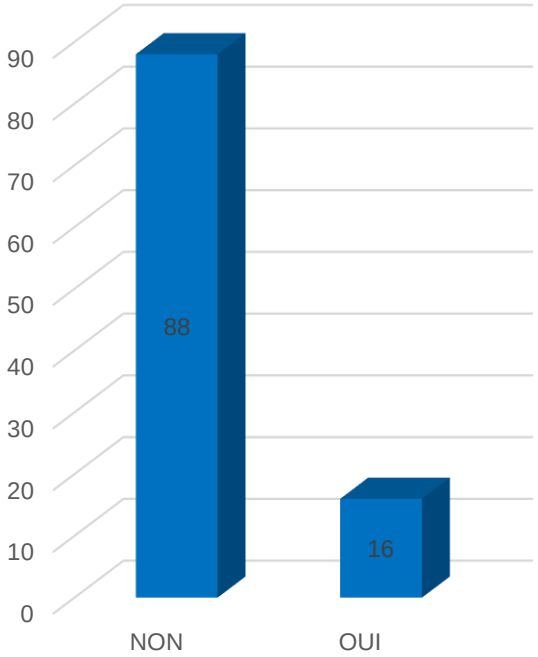
Nombre de CVE par catégorie de produit et score CVSS



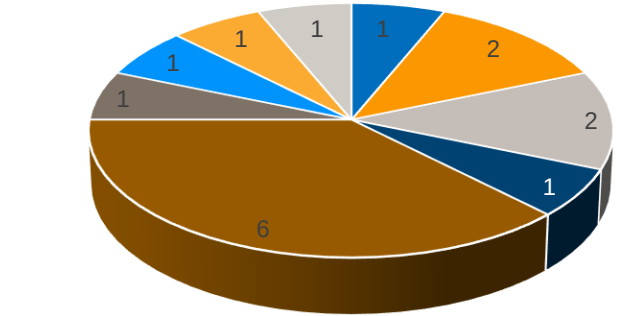


Vulnérabilités exploitées

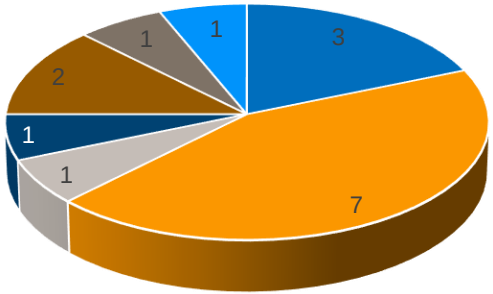
Failles exploitées



Failles exploitées par éditeur



Failles exploitées par type de solution



Les vulnérabilités critiques à surveiller

Cisco ASA et FTD
(CVE-2023-20269)

Contournement de la politique de sécurité

Exploitée

Un attaquant non authentifié peut contourner la politique de sécurité et mener des attaques par force brute.

Recommandations : Appliquez les bonnes pratiques indiquées par l'éditeur.

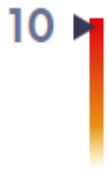
Google Chrome / WebP
(CVE-2023-4863)

Exécution de code arbitraire

Exploitée

Un attaquant non authentifié peut exécuter du code arbitraire sur le système de la victime si elle consulte un site web spécifiquement forgé.

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



Progress Software WS_FTP
(CVE-2023-40044)

Exécution de code arbitraire

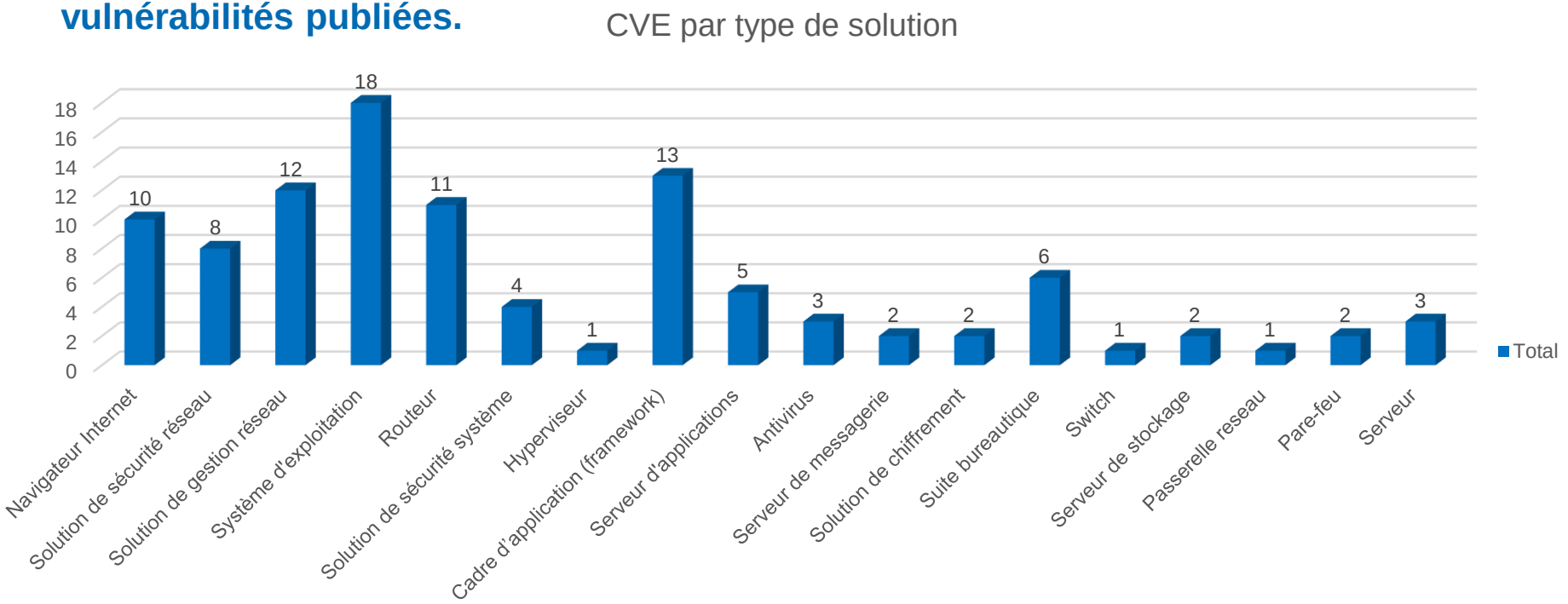
Exploitée

En envoyant des requêtes forgées, un attaquant non authentifié peut exécuter du code sur le serveur WS_FTP.

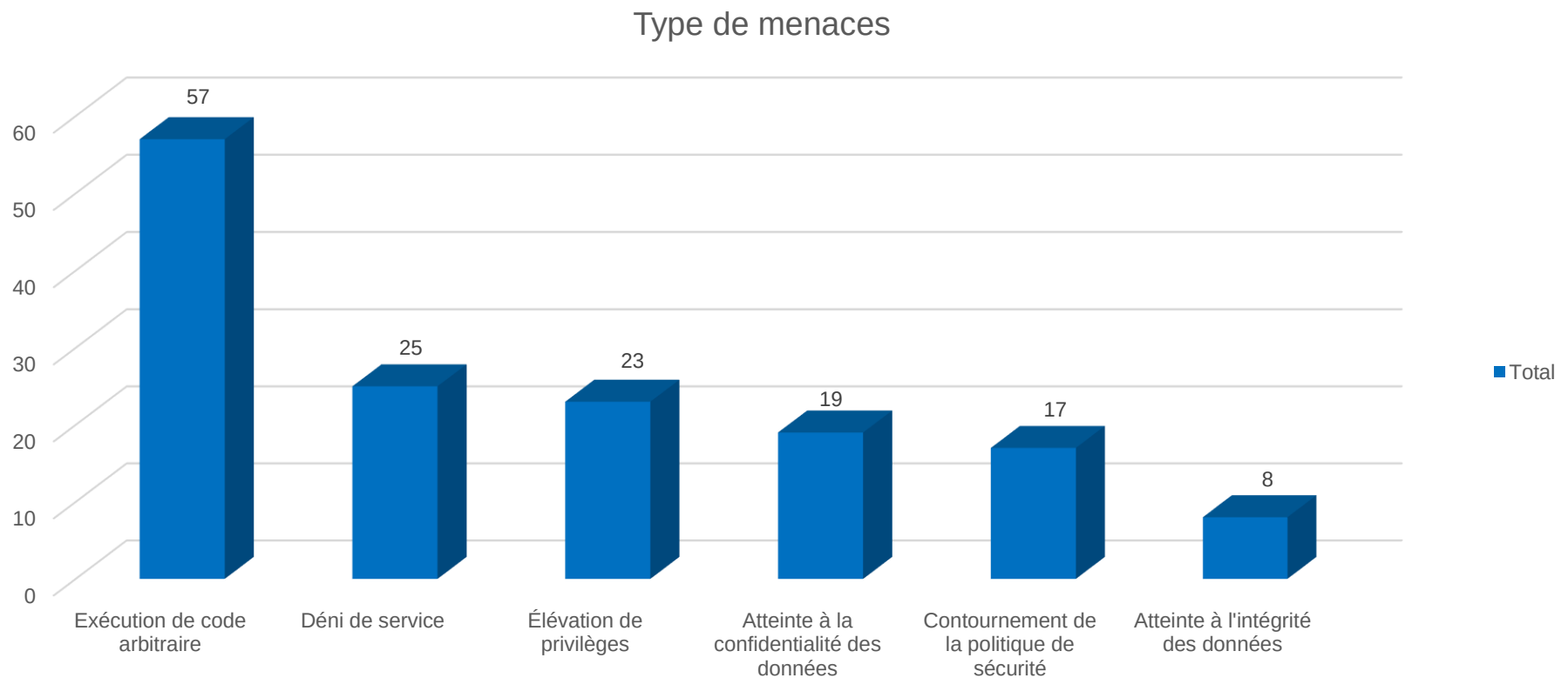
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solution vulnérables

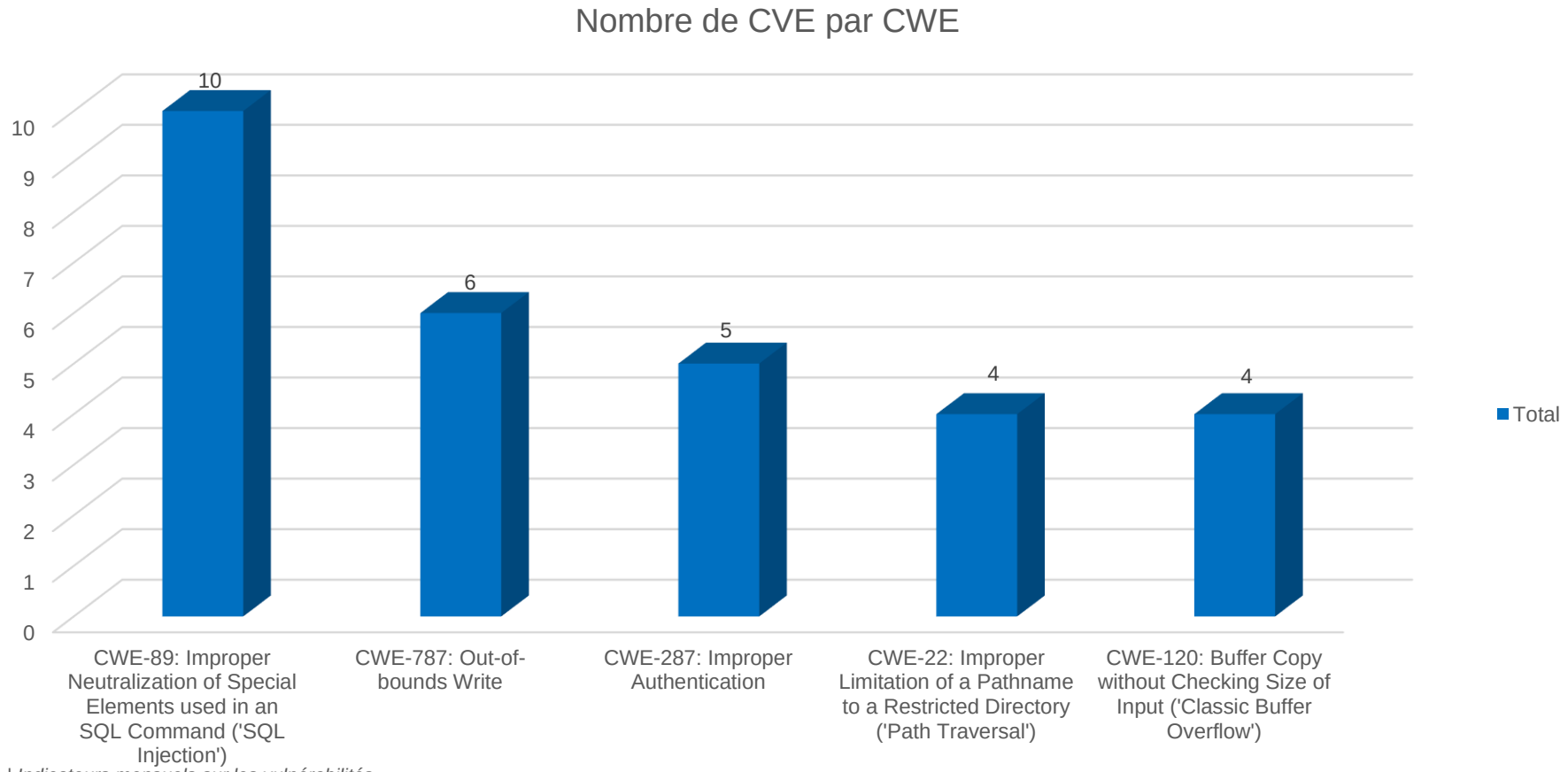
Les cadres d'applications, les solutions de gestion réseau et les systèmes d'exploitation sont les principaux types d'équipements affectés par les vulnérabilités publiées.



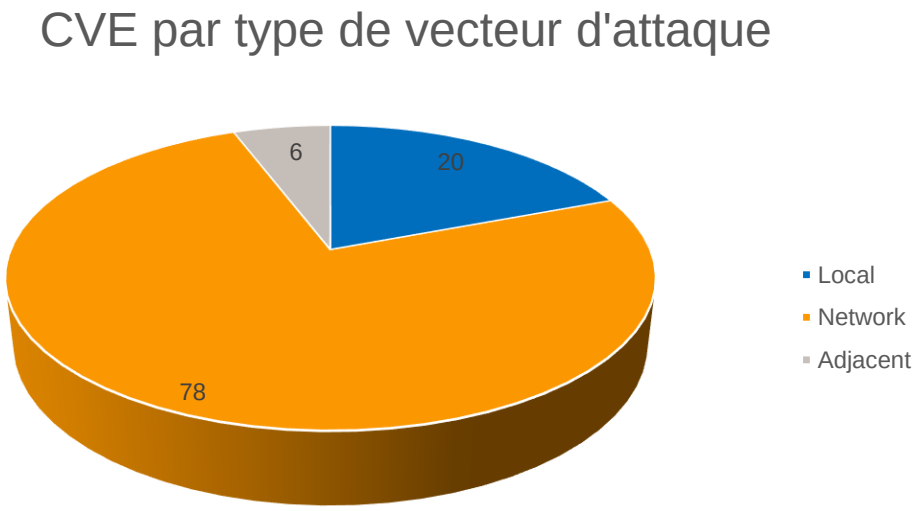
Types de menaces

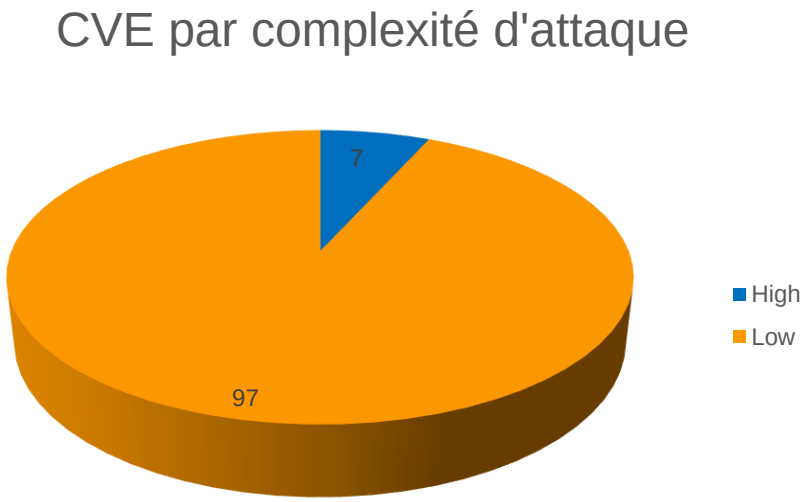


TOP 5 des failles selon le référentiel CWE



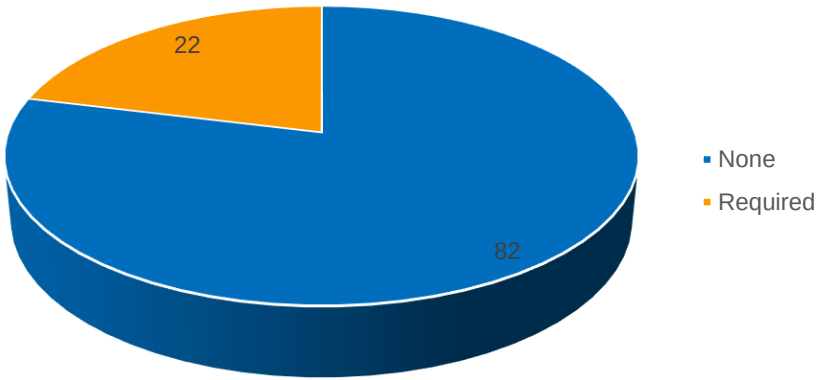
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



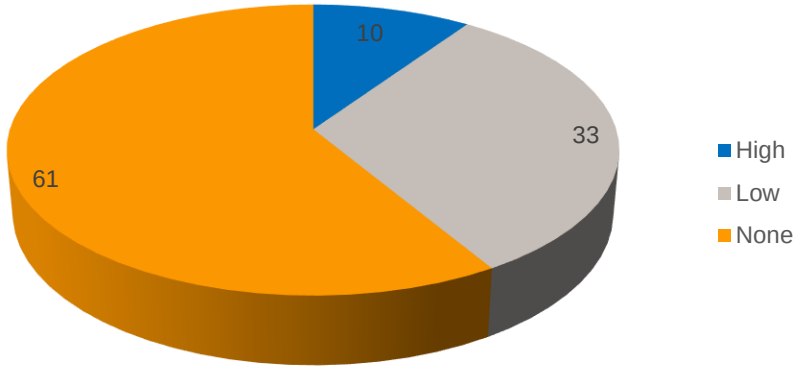


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

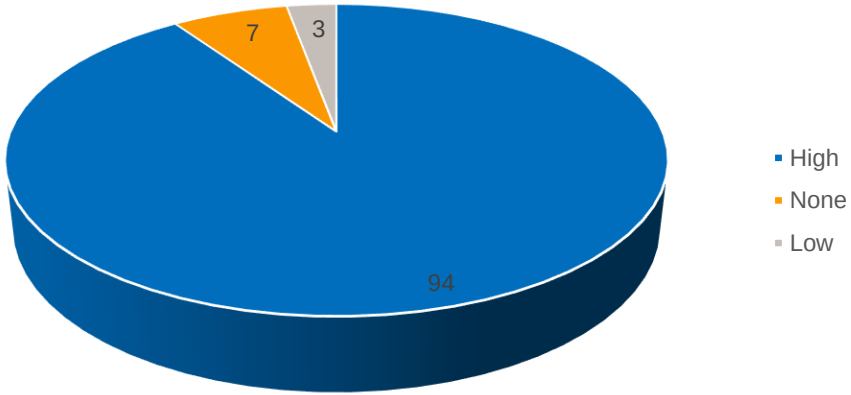
CVE par interaction utilisateur

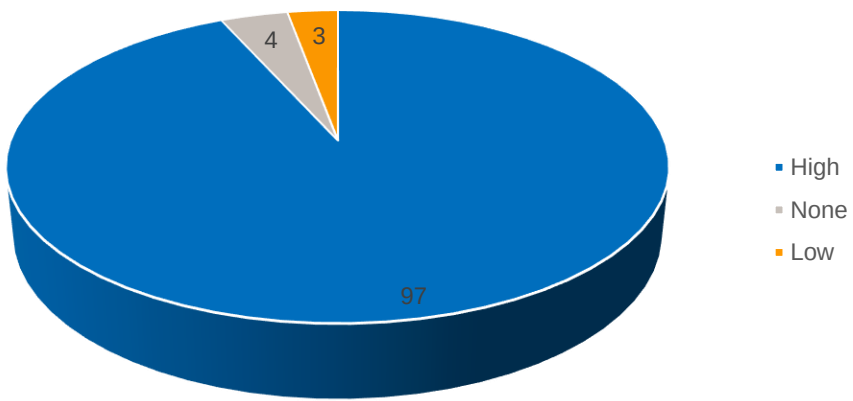


CVE par type de privilège requis

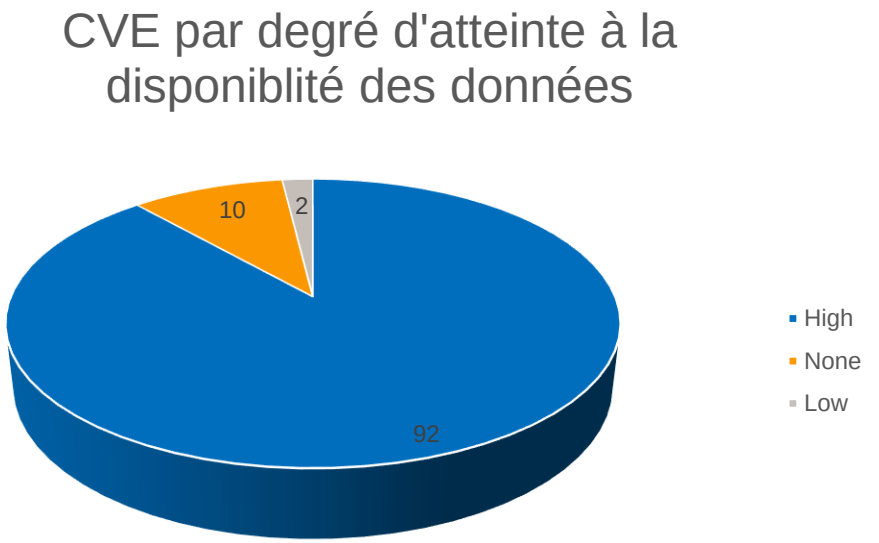


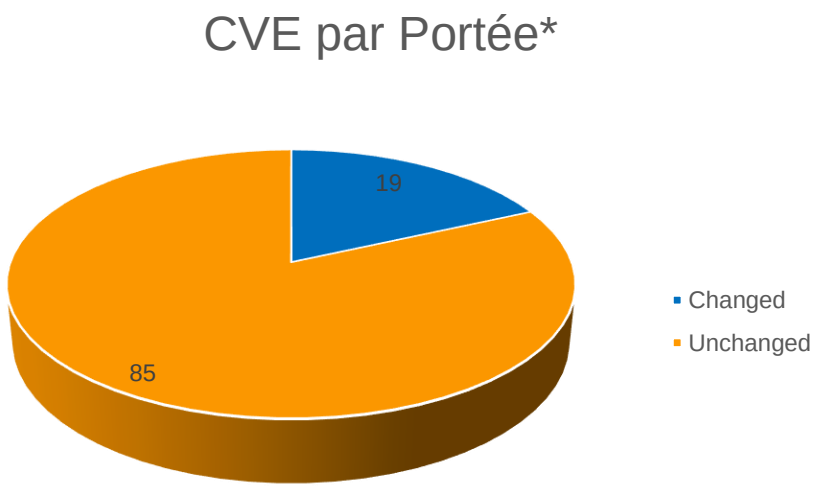
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données





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.