AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

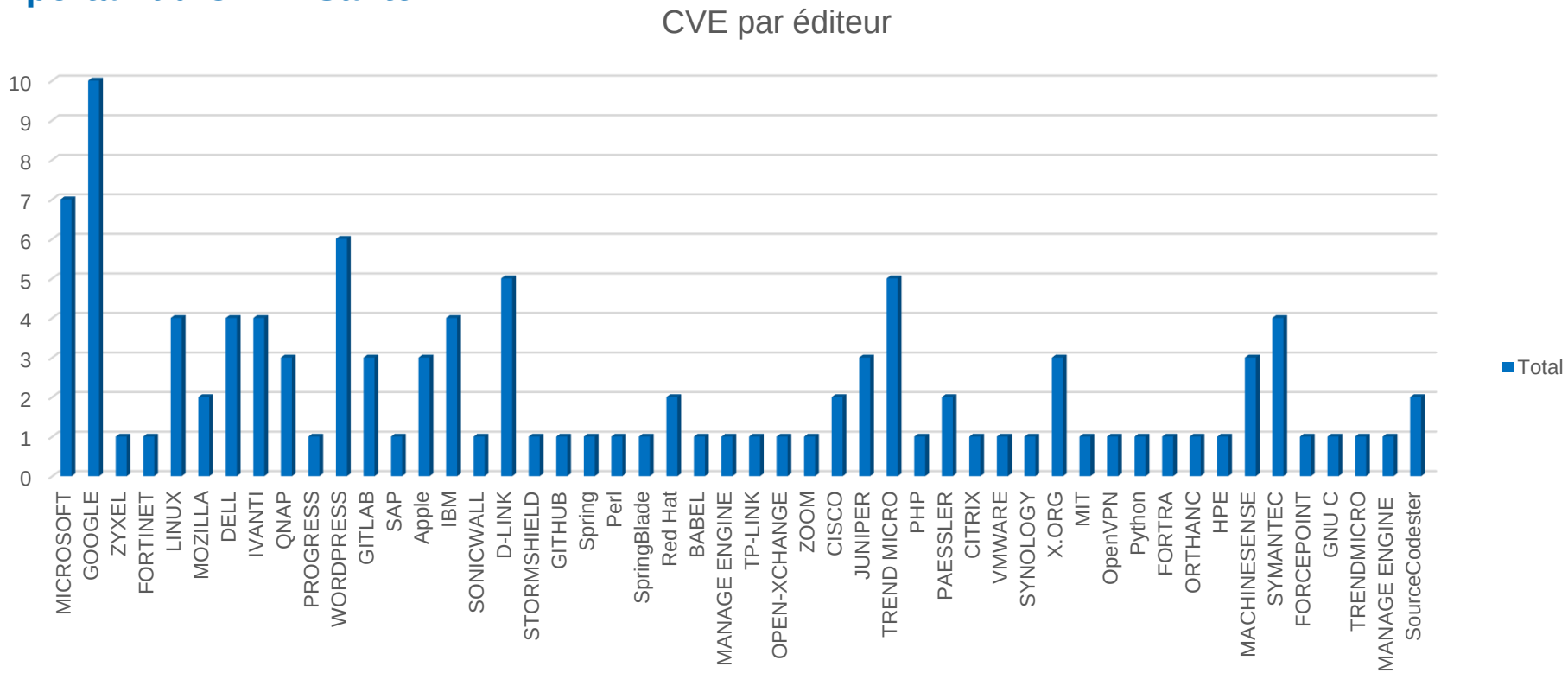
Indicateurs sur la publication des CVE pour le mois de janvier 2024

CERT Santé

Février 2024

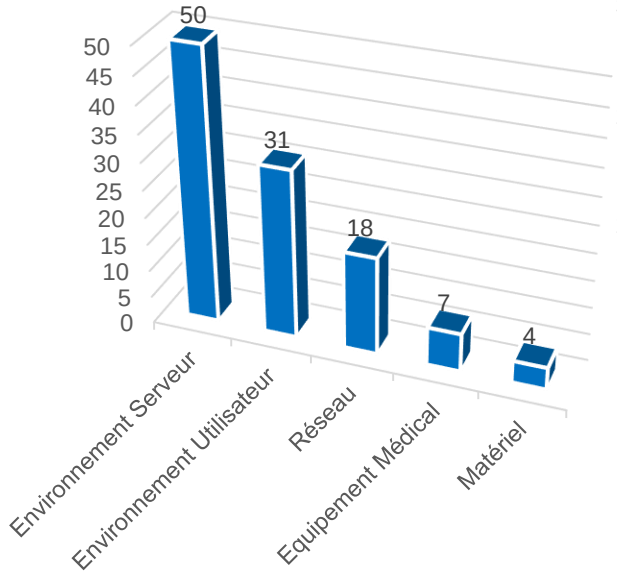
Nombre de CVE par éditeur

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

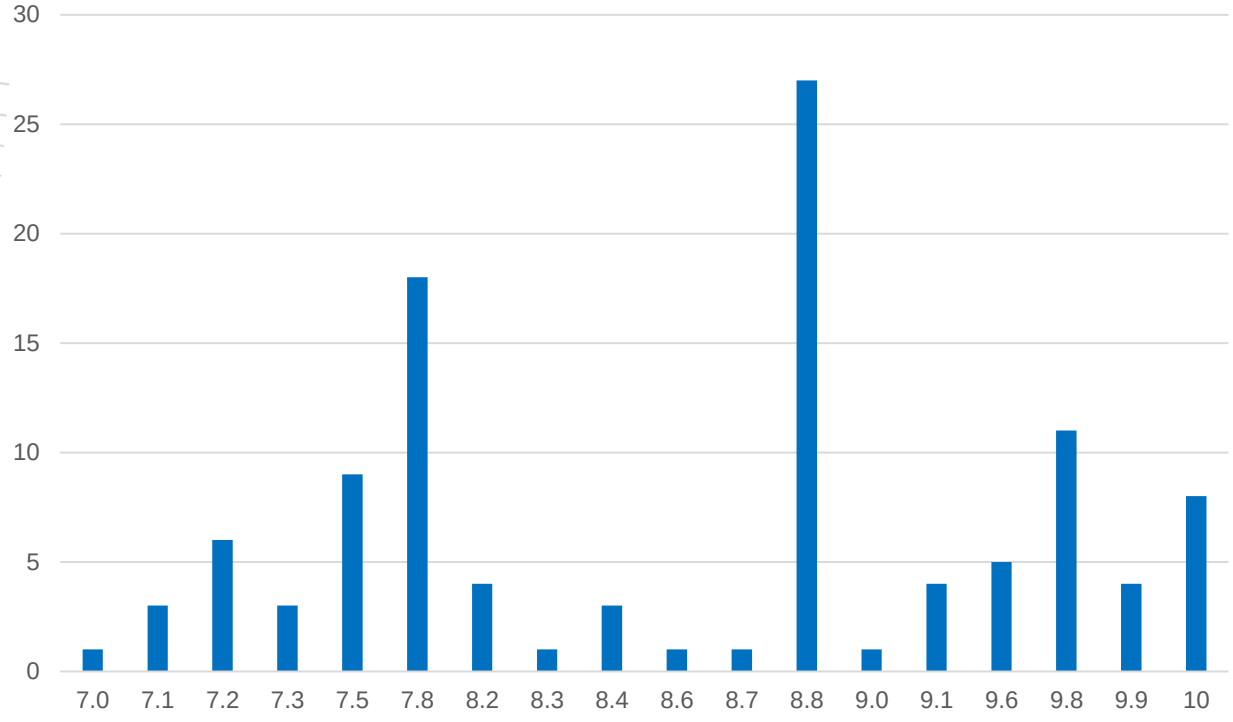


Nombre de CVE par catégorie de produit et score CVSS

CVE par catégorie de solution

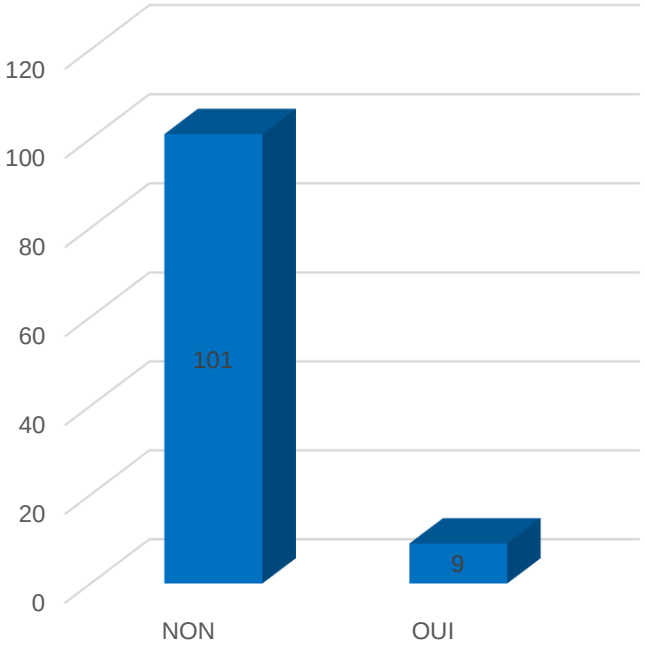


CVE par score CVSS

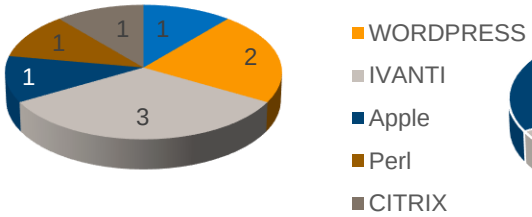


Vulnérabilités exploitées

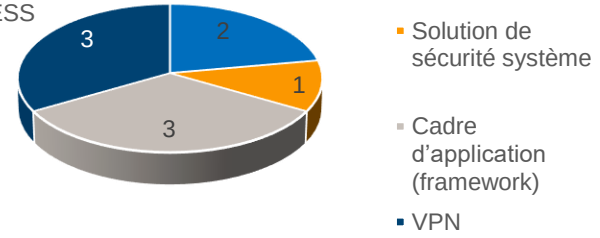
Failles exploitées



Failles exploitées par éditeur



Failles exploitées par type de solution



Les vulnérabilités critiques à surveiller

Ivanti
(CVE-2024-21887)

Exécution de code arbitraire

Exploitée

Une vulnérabilité dans les composants Web du VPN Ivanti Connect Secure (ex-Pulse Secure) et Ivanti Policy Secure permet à un attaquant authentifié d'exécuter du code arbitraire.

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

Apple Webkit
(CVE-2024-23222)

Exécution de code arbitraire

Exploitée

Une vulnérabilité dans le WebKit d'Apple permet à un attaquant non authentifié d'exécuter du code arbitraire, en persuadant une victime de consulter un site spécifiquement forgé.

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

CITRIX
(CVE-2023-6549)

Déni de service

Exploitée

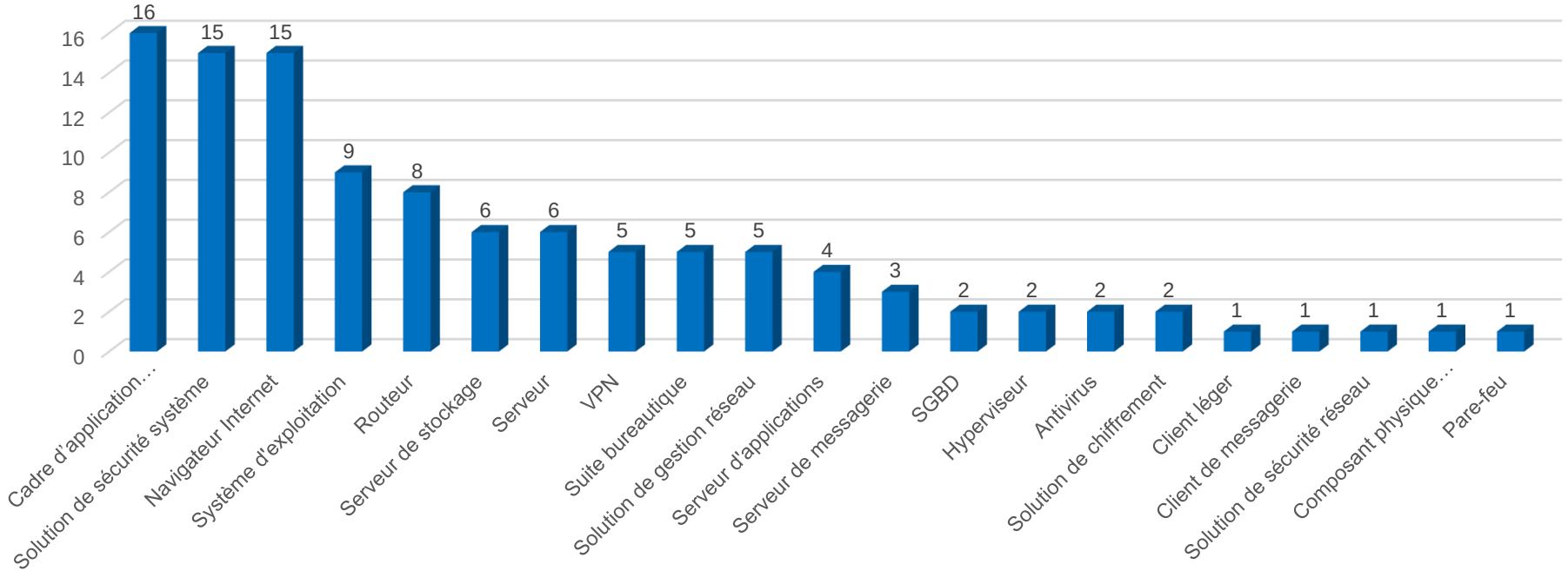
Un défaut dans Citrix NetScaler permet à un attaquant non authentifié, lorsque ces produits sont configurés en passerelle ou en serveur virtuel AAA, de provoquer un déni de service.

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

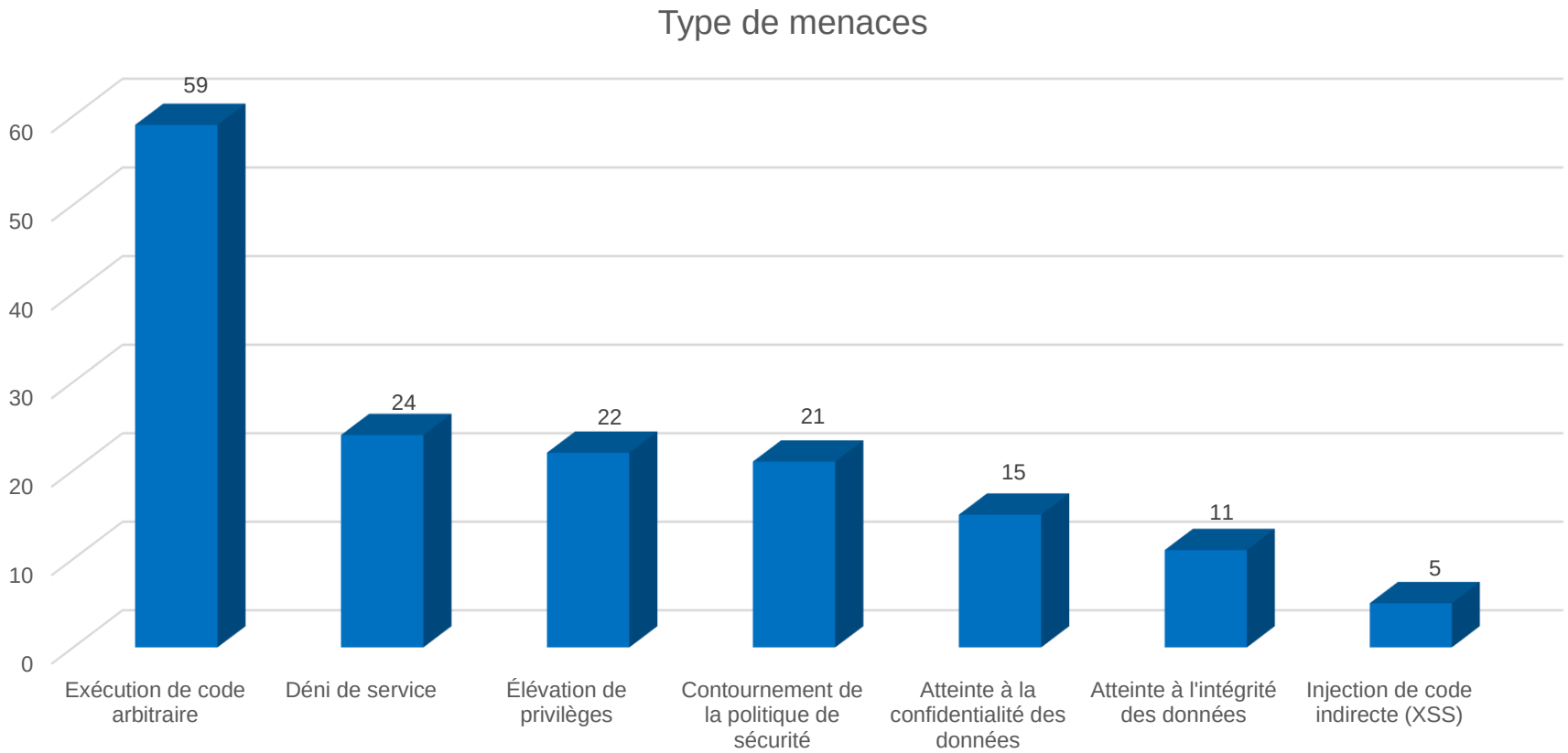
Types de solutions vulnérables

Les cadres d'application (framework), les solutions de sécurité système et les navigateurs internet sont les principaux types d'équipements affectés par les vulnérabilités publiées.

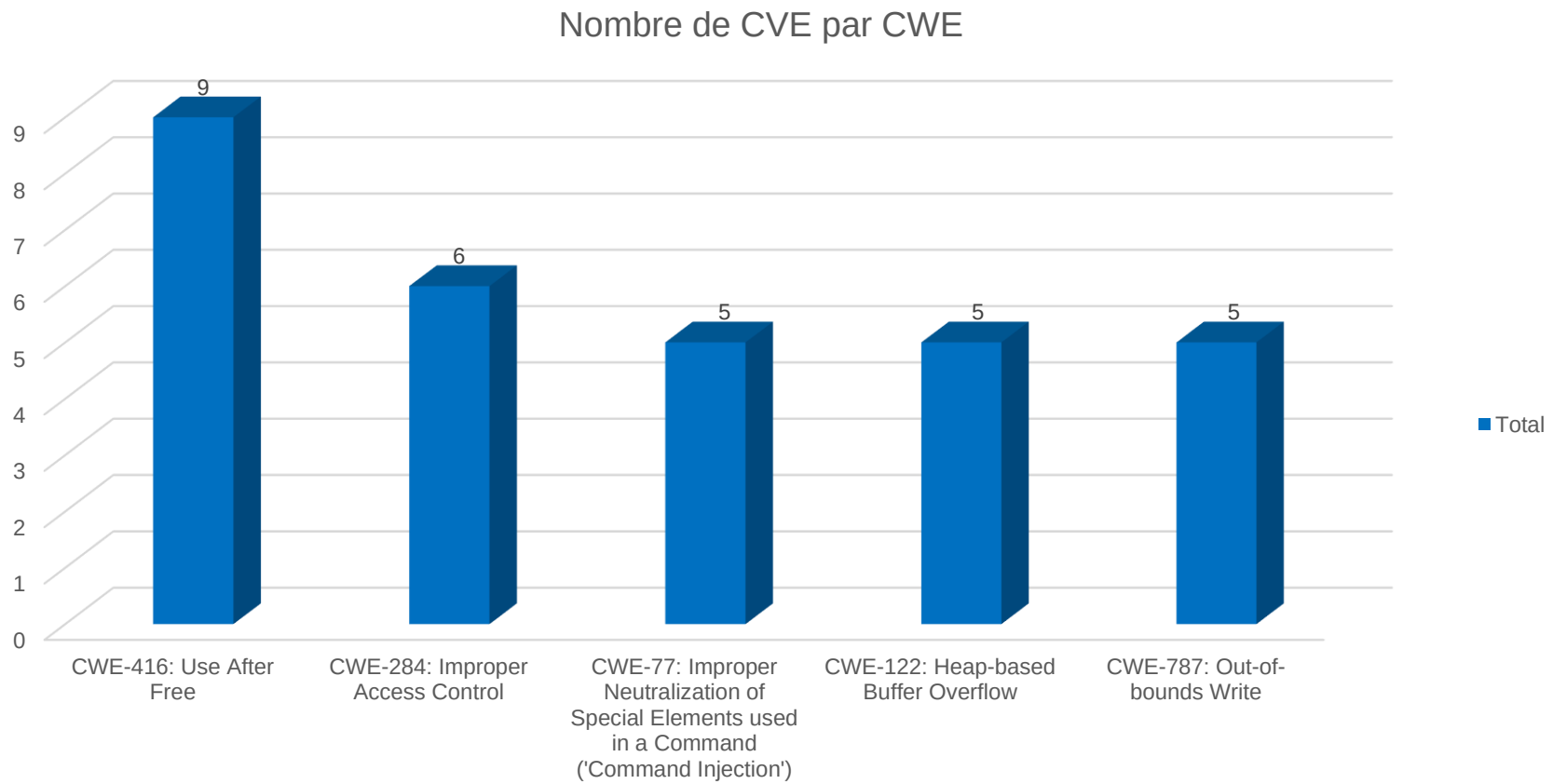
CVE par type de solution



Types de menaces

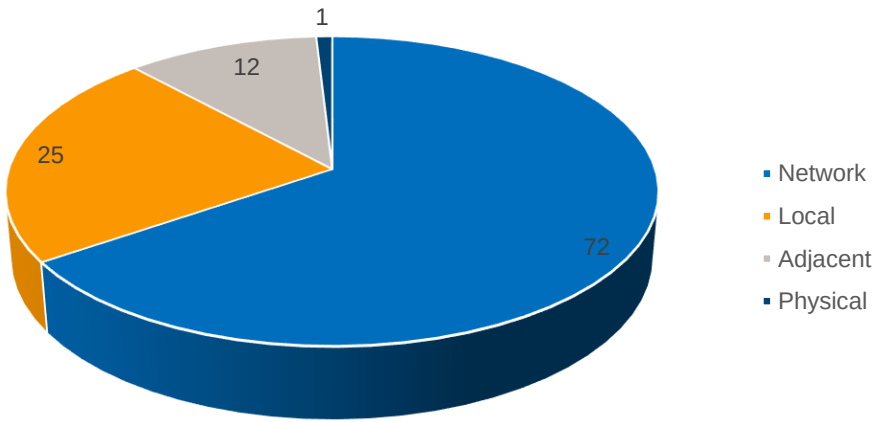


TOP 5 des failles selon le référentiel CWE

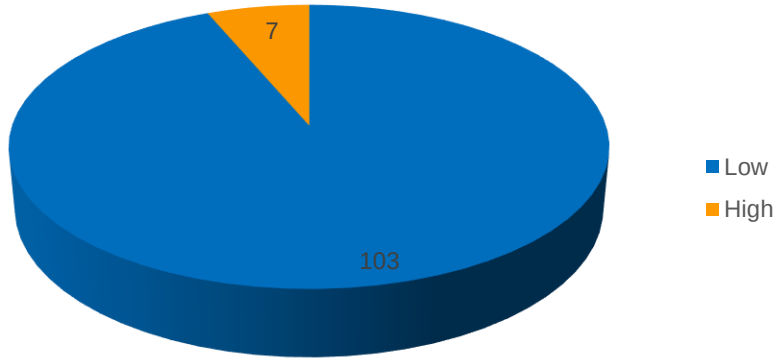


Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque

CVE par type de vecteur d'attaque

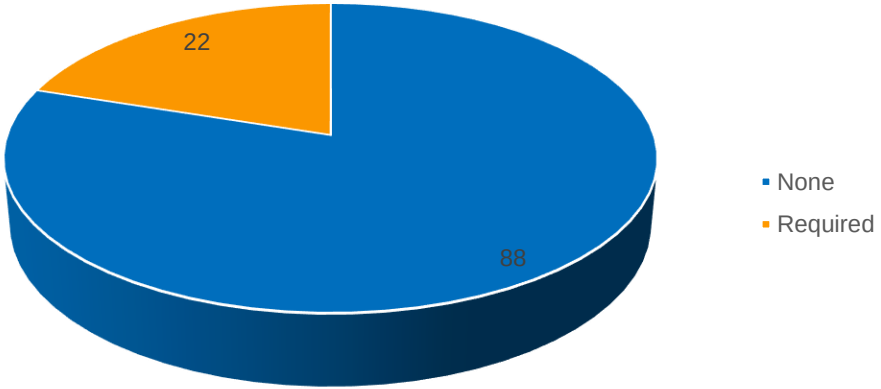


CVE par complexité d'attaque

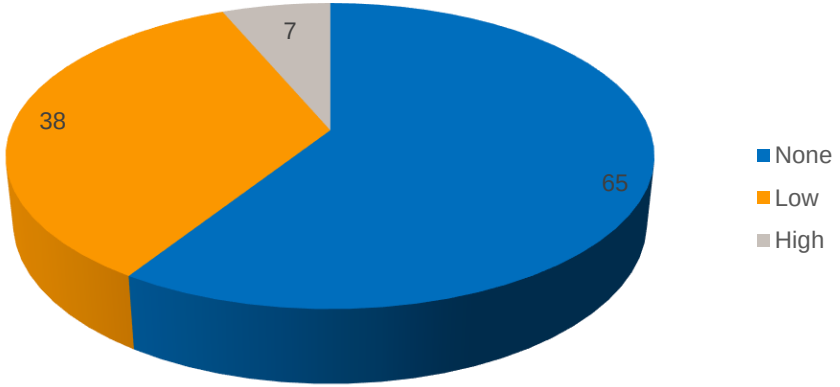


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

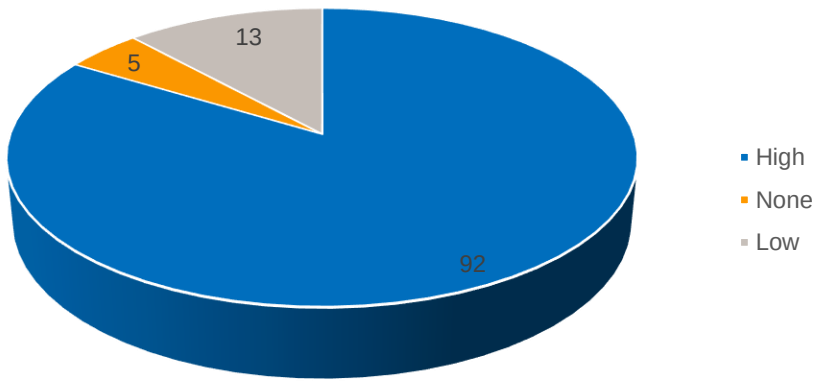


CVE par type de privilège requis

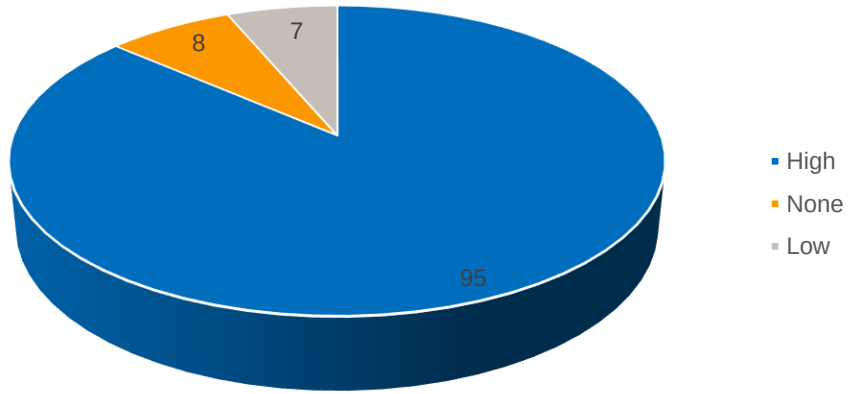


Nombre de CVE selon l’impact sur l’intégrité et sur la confidentialité des données

CVE par degré d'atteinte à l'intégrité des données

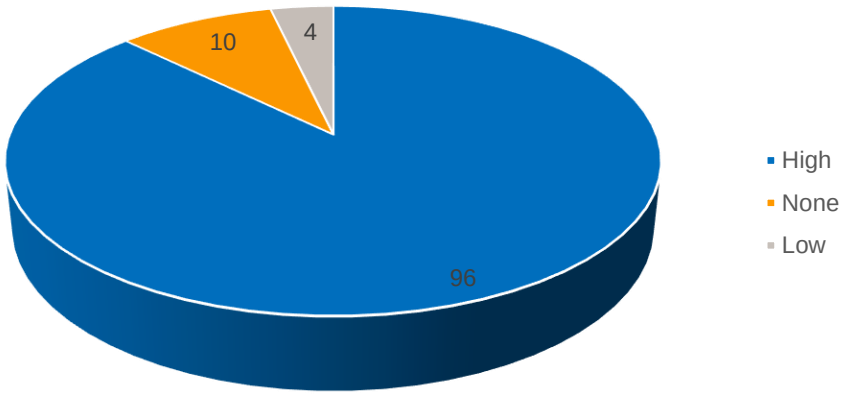


CVE par degré d'atteinte à la confidentialité des données

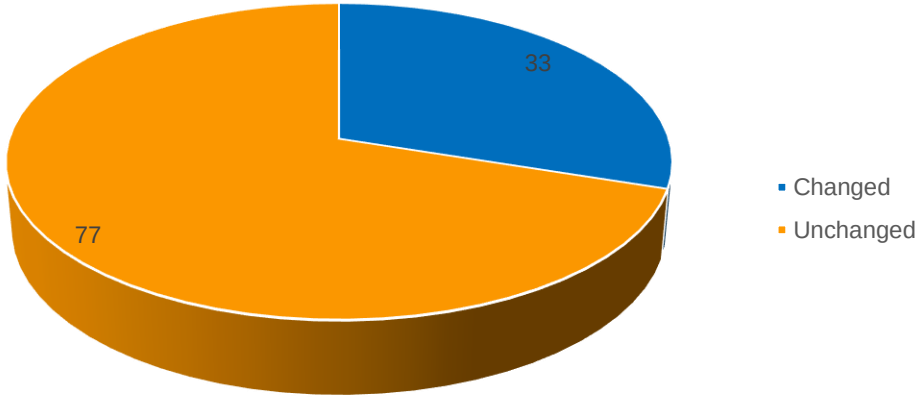


Nombre de CVE selon l'impact sur la disponibilité des données et la portée

CVE par degré d'atteinte à la disponiblité des données



CVE par 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.