AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

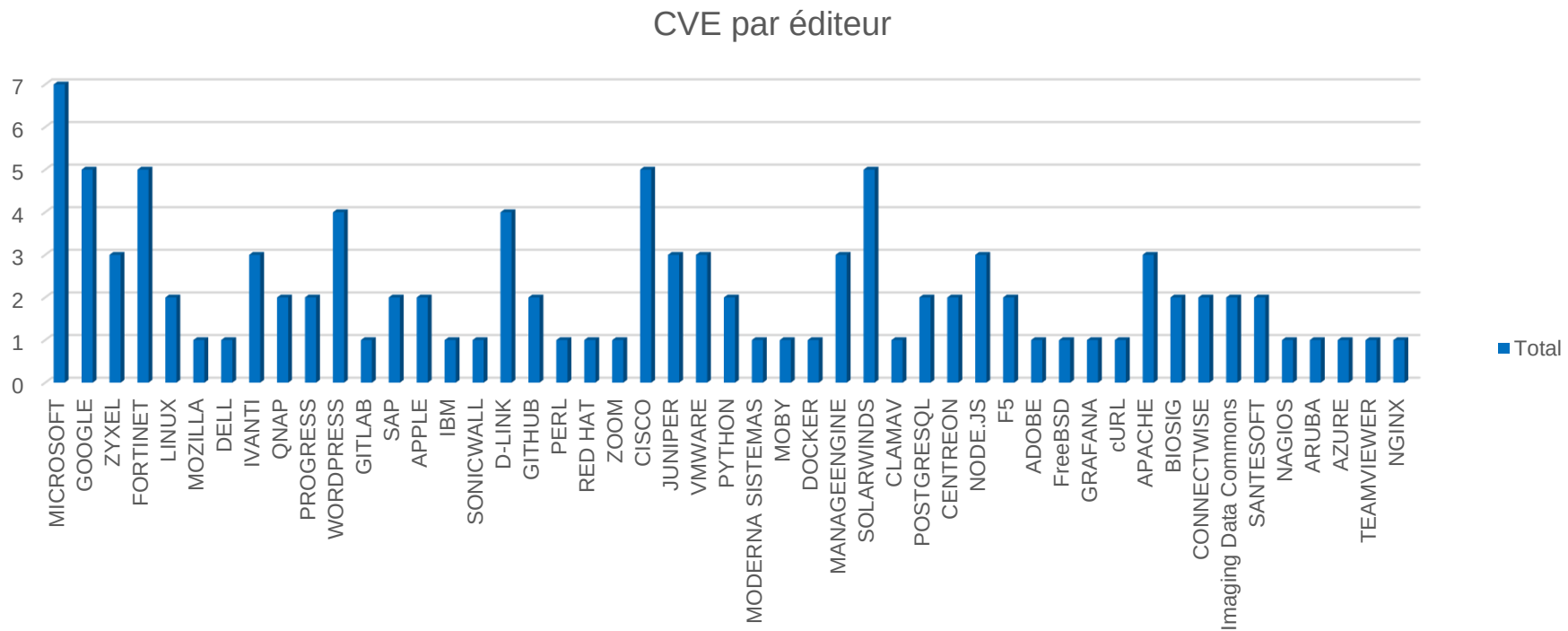
Indicateurs sur la publication des CVE pour le mois de février 2024

CERT Santé

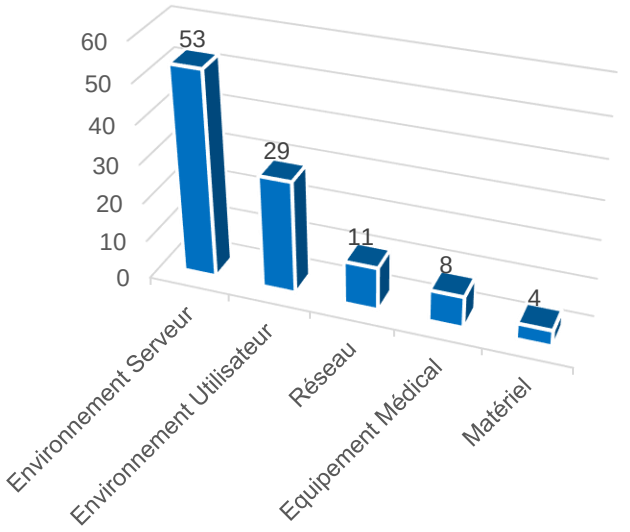
mars 2024

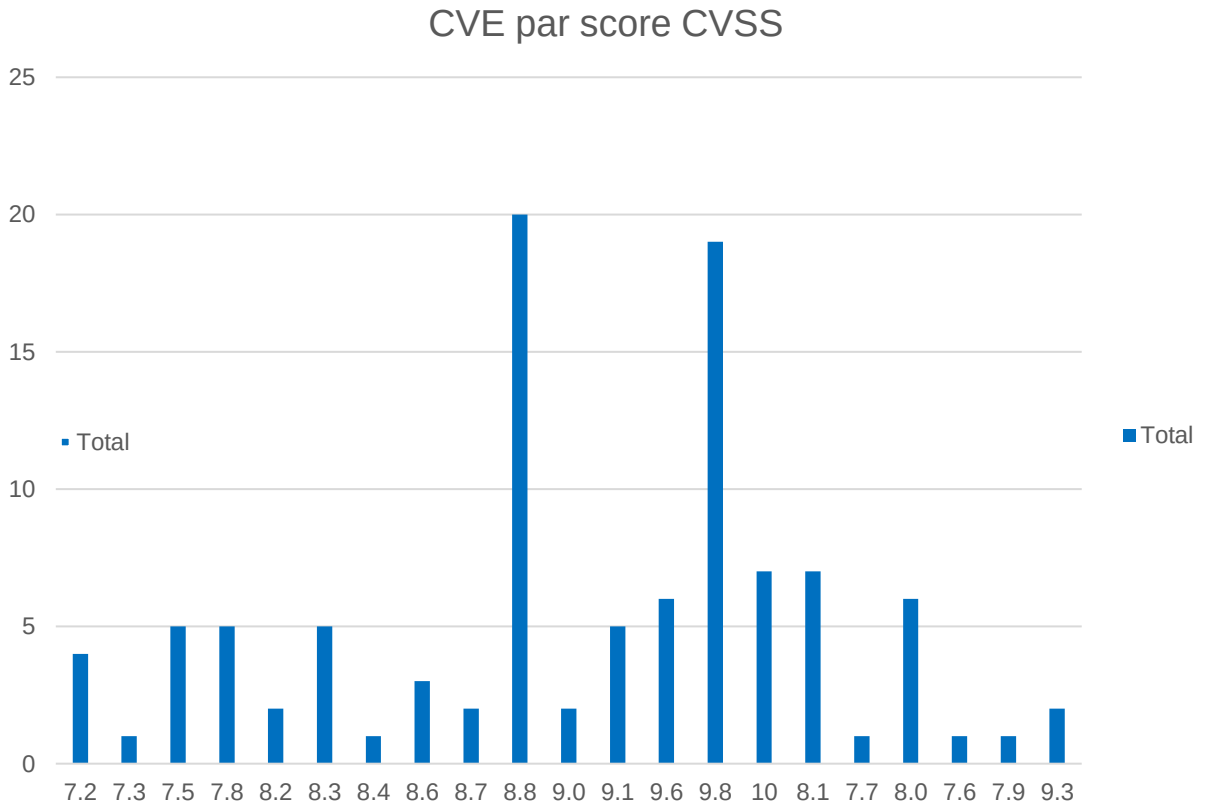
Nombre de CVE par éditeur

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

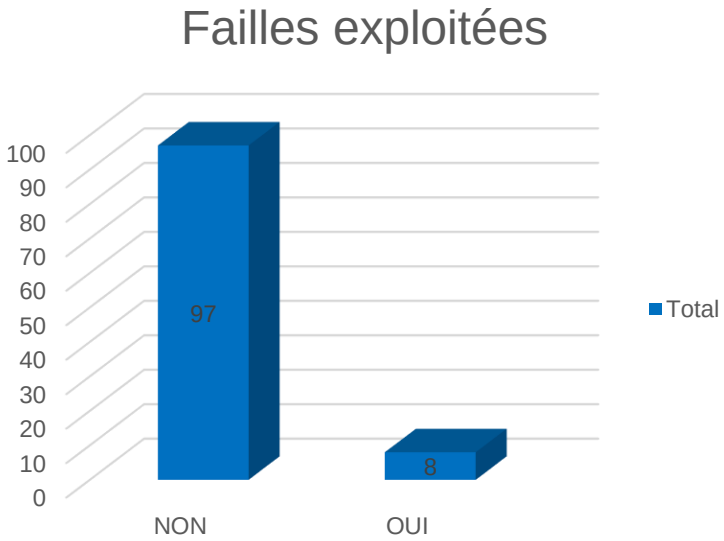


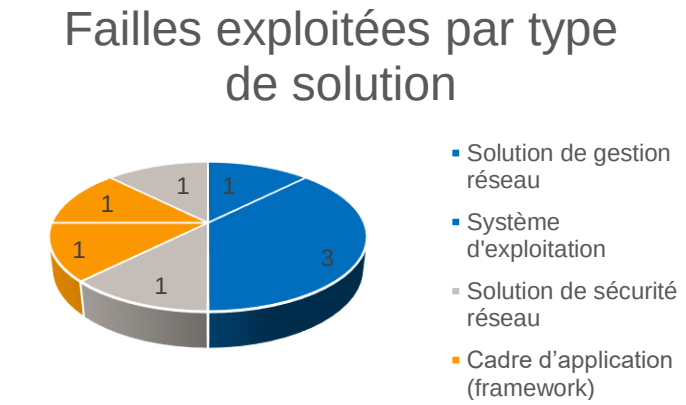
Nombre de CVE par catégorie de produit et score CVSS

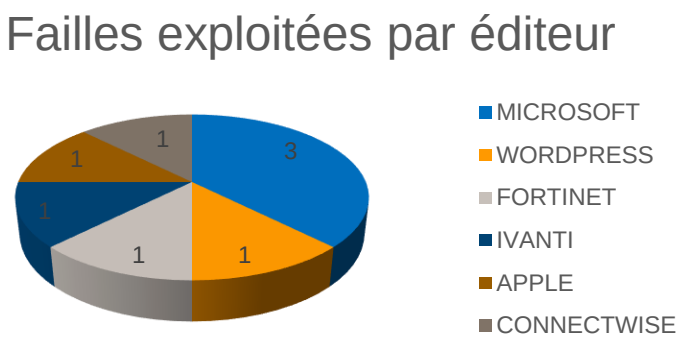




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

10

ConnectWise ScreenConnect

(CVE-2024-1709)

Contournement de la politique de sécurité

Exploitée

Un défaut de contrôle d'authentification dans ConnectWise SmartConnect permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, de créer des comptes administrateur.

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

9.8

Microsoft

(CVE-2024-21413)

Exécution de code arbitraire

Exploitée

Un défaut de contrôle des données envoyées par l'utilisateur dans Outlook via Office permet à un attaquant non authentifié, en contournant le protocole Protected View, d'exécuter du code arbitraire.

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

9.8

Fortinet

(CVE-2024-21762)

Exécution de code arbitraire

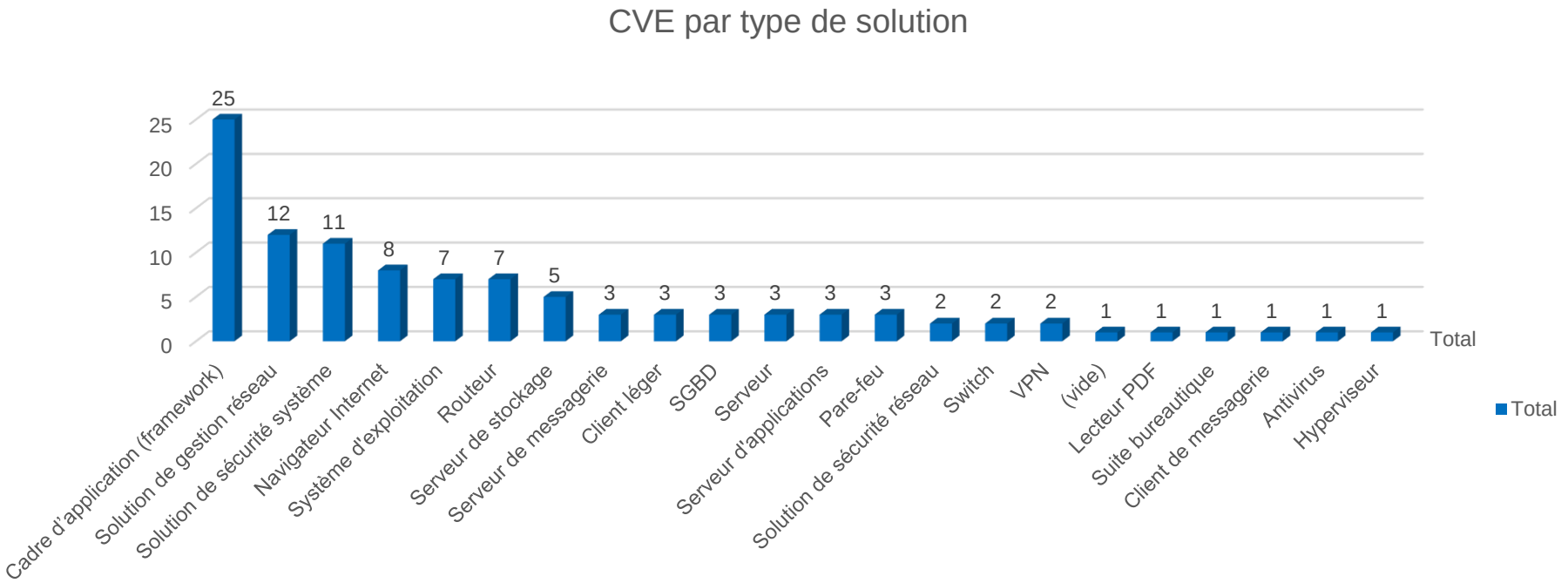
Exploitée

Un défaut de vérification de données saisies par l'attaquant dans le *SSL-VPN* de FortiOS permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire.

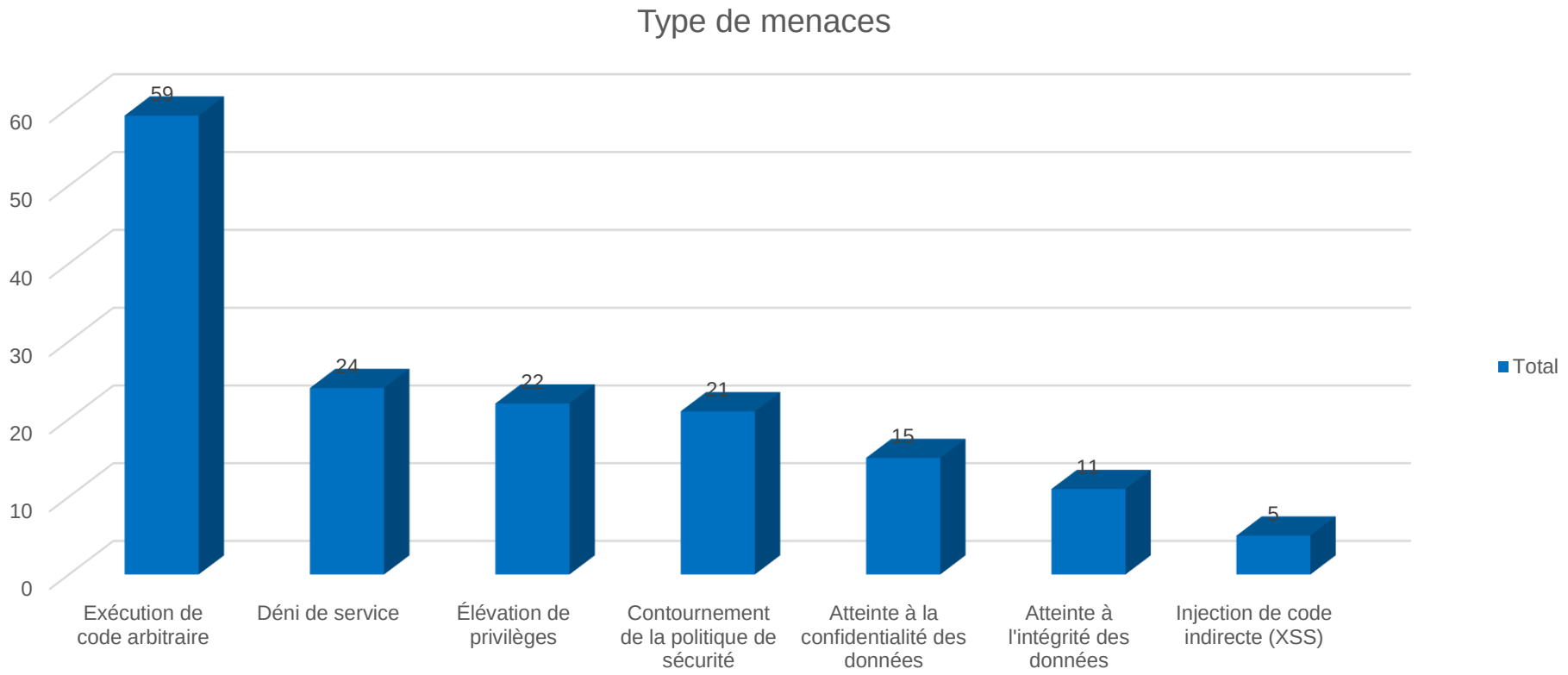
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

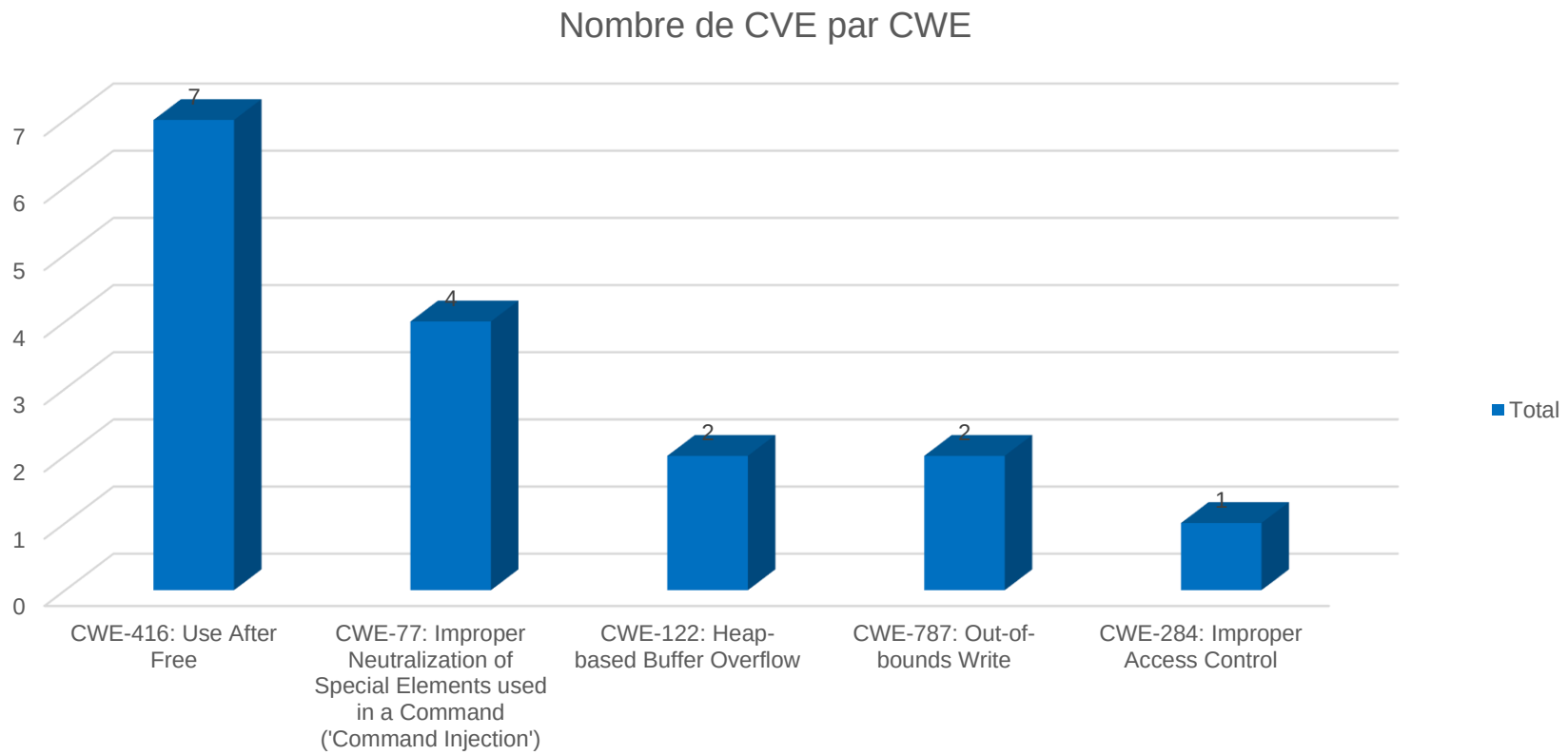
Les cadres d'application (framework), les solutions de gestion réseau et les solutions de sécurité système sont les principaux types d'équipements affectés par les vulnérabilités publiées.



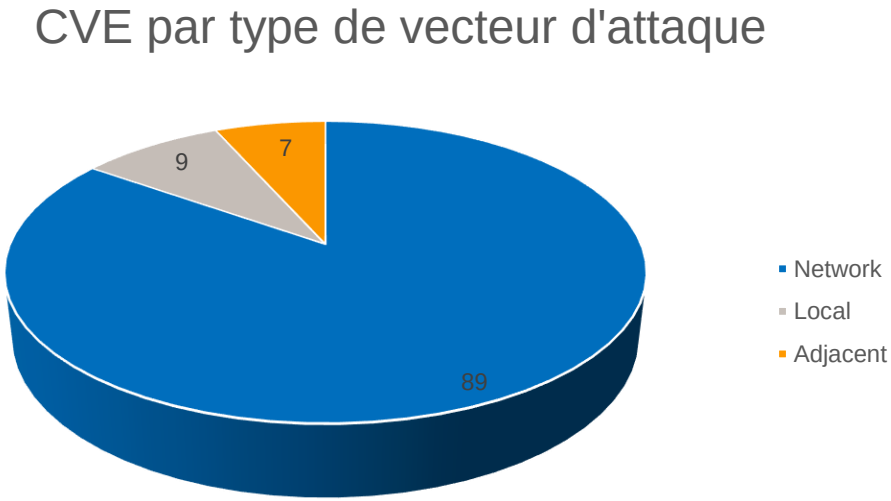
Types de menaces

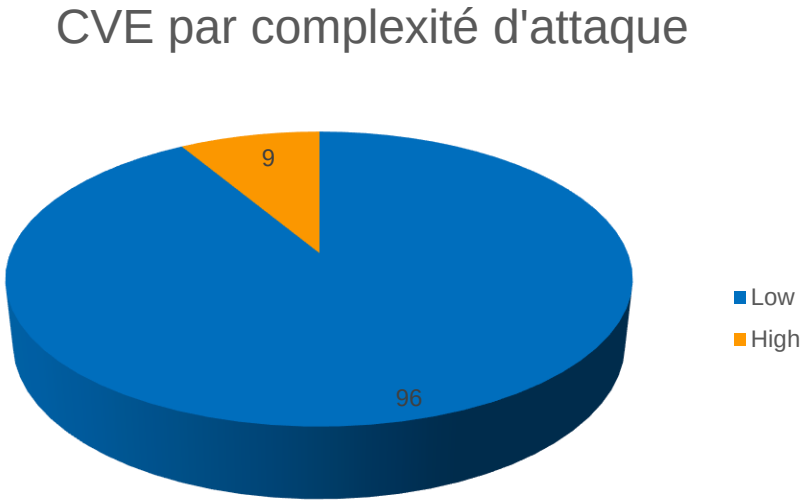


TOP 5 des failles selon le référentiel CWE



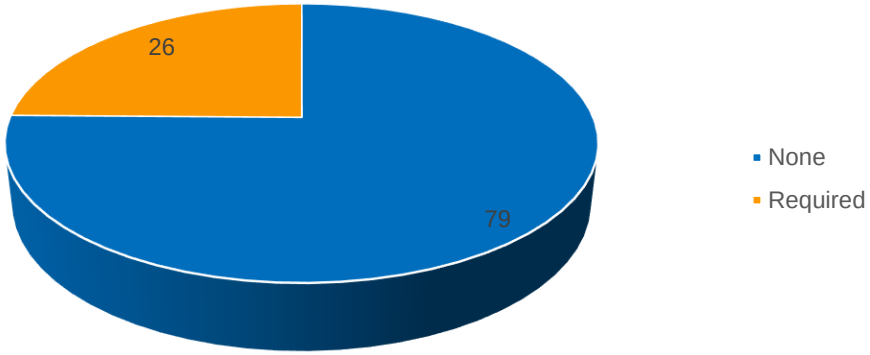
Nombre de CVE selon le vecteur d’attaque et la complexité de l’attaque



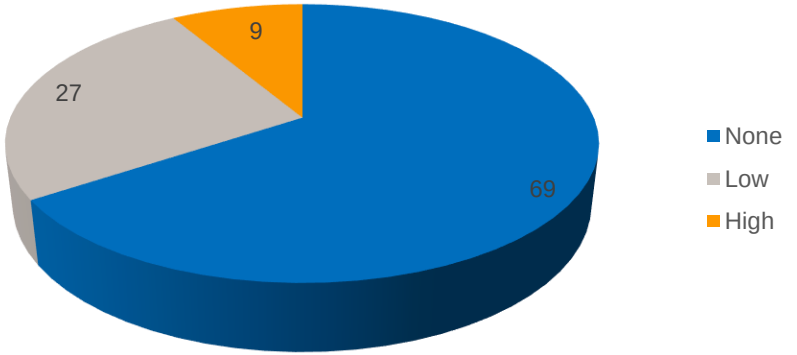


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

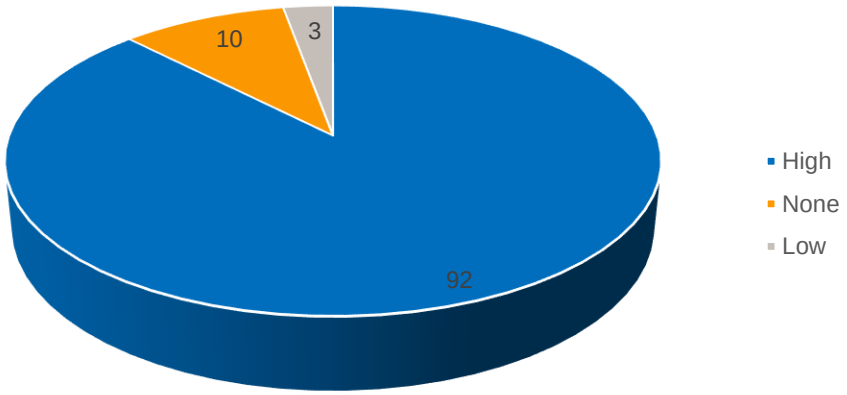


CVE par type de privilège requis

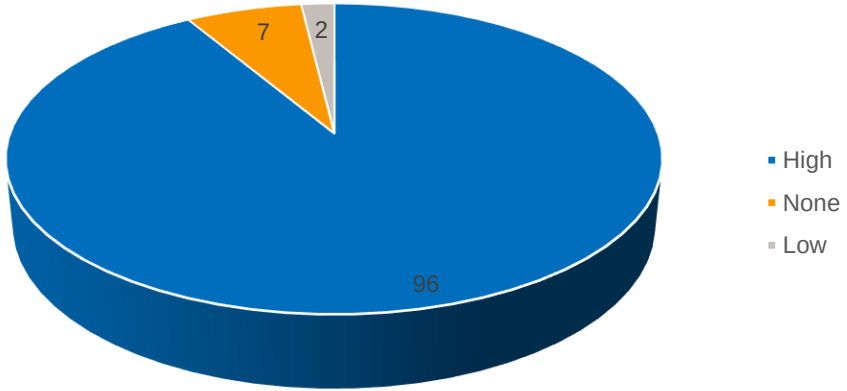


Nombre de CVE selon l’impact sur l’intégrité et sur la confidentialité des données

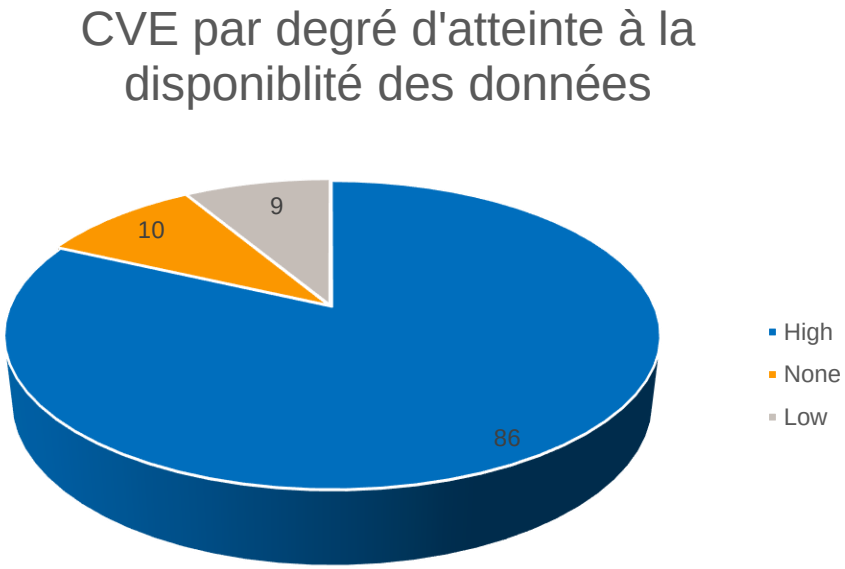
CVE par degré d'atteinte à l'intégrité des données

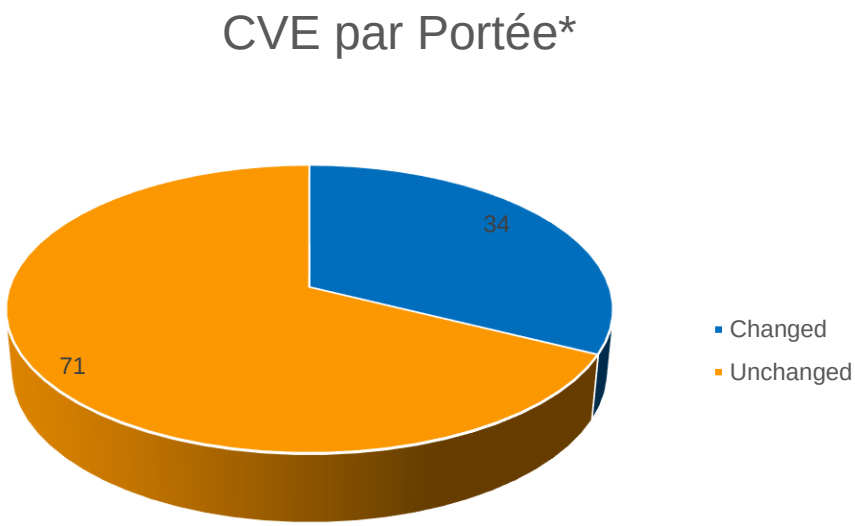


CVE par degré d'atteinte à la confidentialité des données



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





*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.