AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

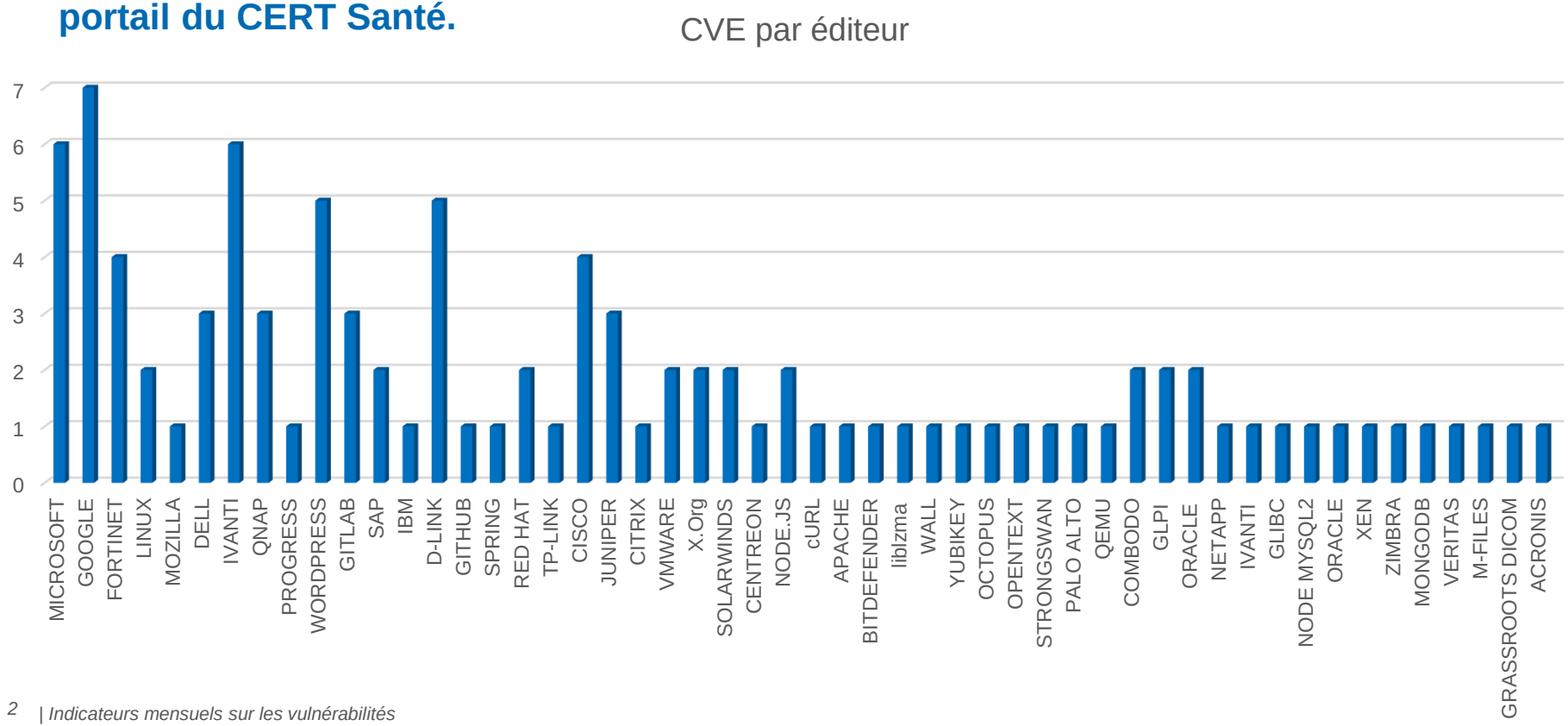
Indicateurs sur la publication des CVE pour le mois d'avril 2024

CERT Santé

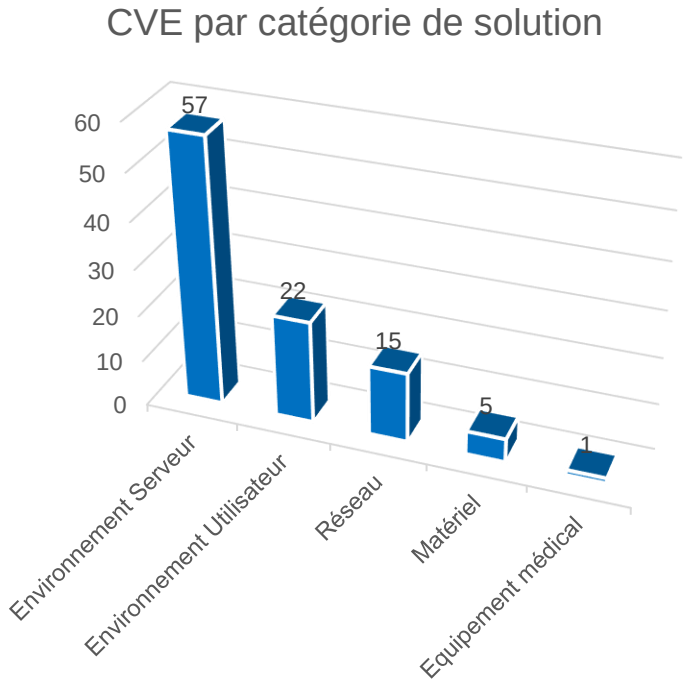
mai 2024

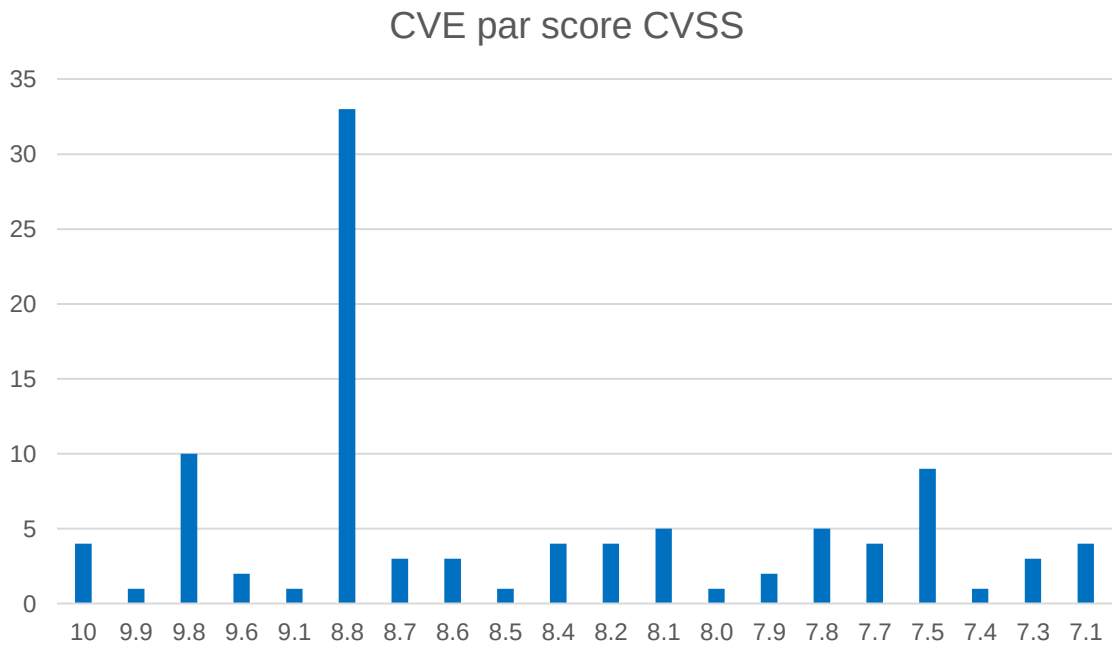
Nombre de CVE par éditeur

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

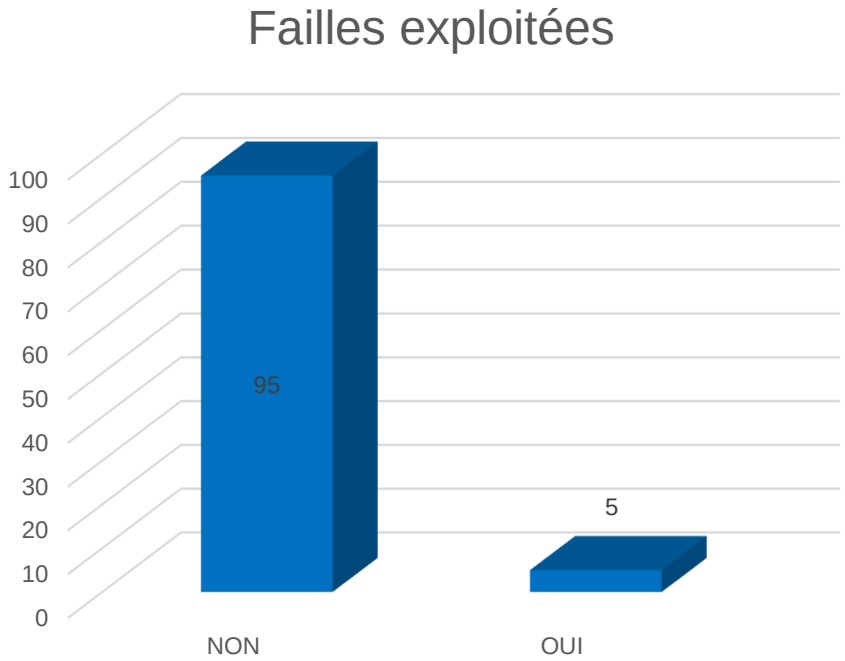


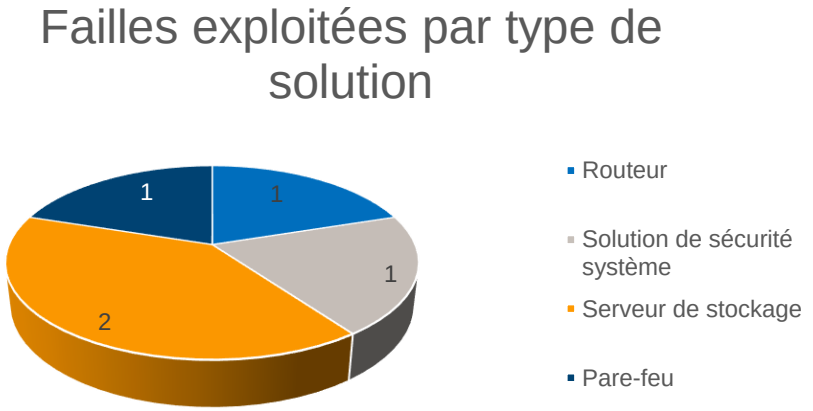
Nombre de CVE par catégorie de produit et score CVSS





Vulnérabilités exploitées





Les vulnérabilités critiques à surveiller

10

Palo Alto
(CVE-2024-3400)

Exécution de code arbitraire

Exploitée

Une injection de commande dans la fonctionnalité *GlobalProtect* de PAN-OS permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire avec les privilèges *root*.

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

10

liblzma
(CVE-2024-3094)

Exécution de code arbitraire

La présence d'une porte dérobée dans la librairie liblzma permet à un attaquant non authentifié, en envoyant des requêtes SSH, de prendre contrôle de l'appareil et d'exécuter du code arbitraire.

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

8.6

Cisco
(CVE-2024-20353)

Déni de service

Exploitée

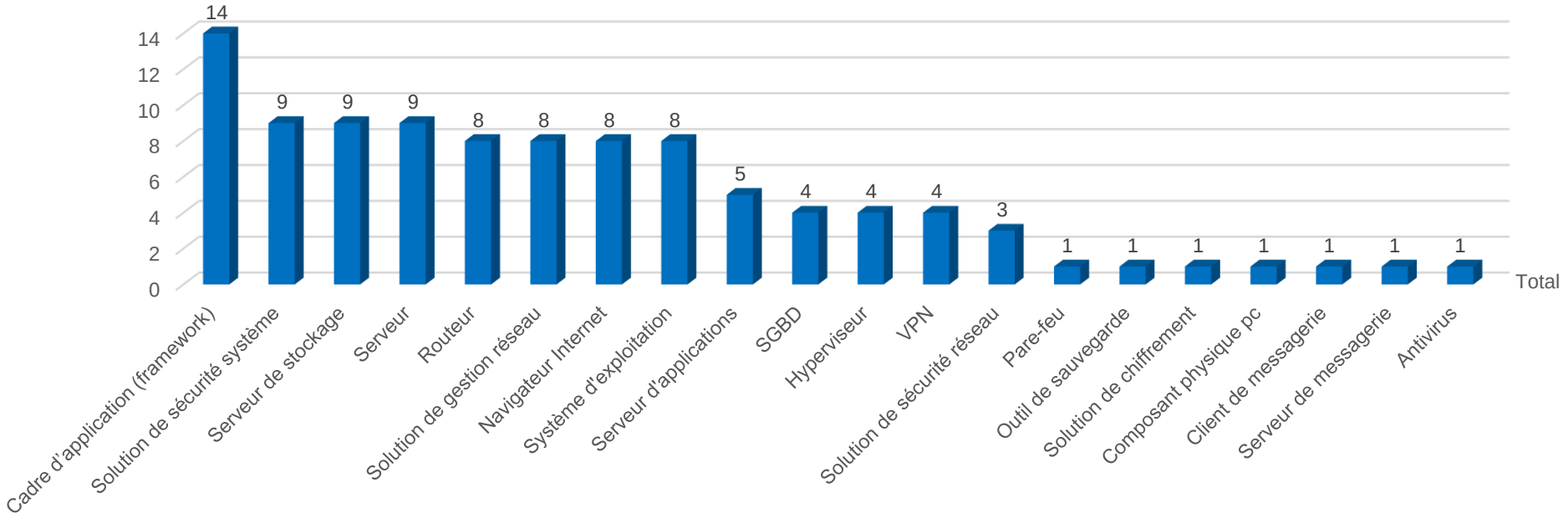
Un défaut de contrôle des erreurs dans l'en-tête HTTP des serveurs de gestion Web et VPN de Cisco ASA et FTD permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, de provoquer un déni de service.

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

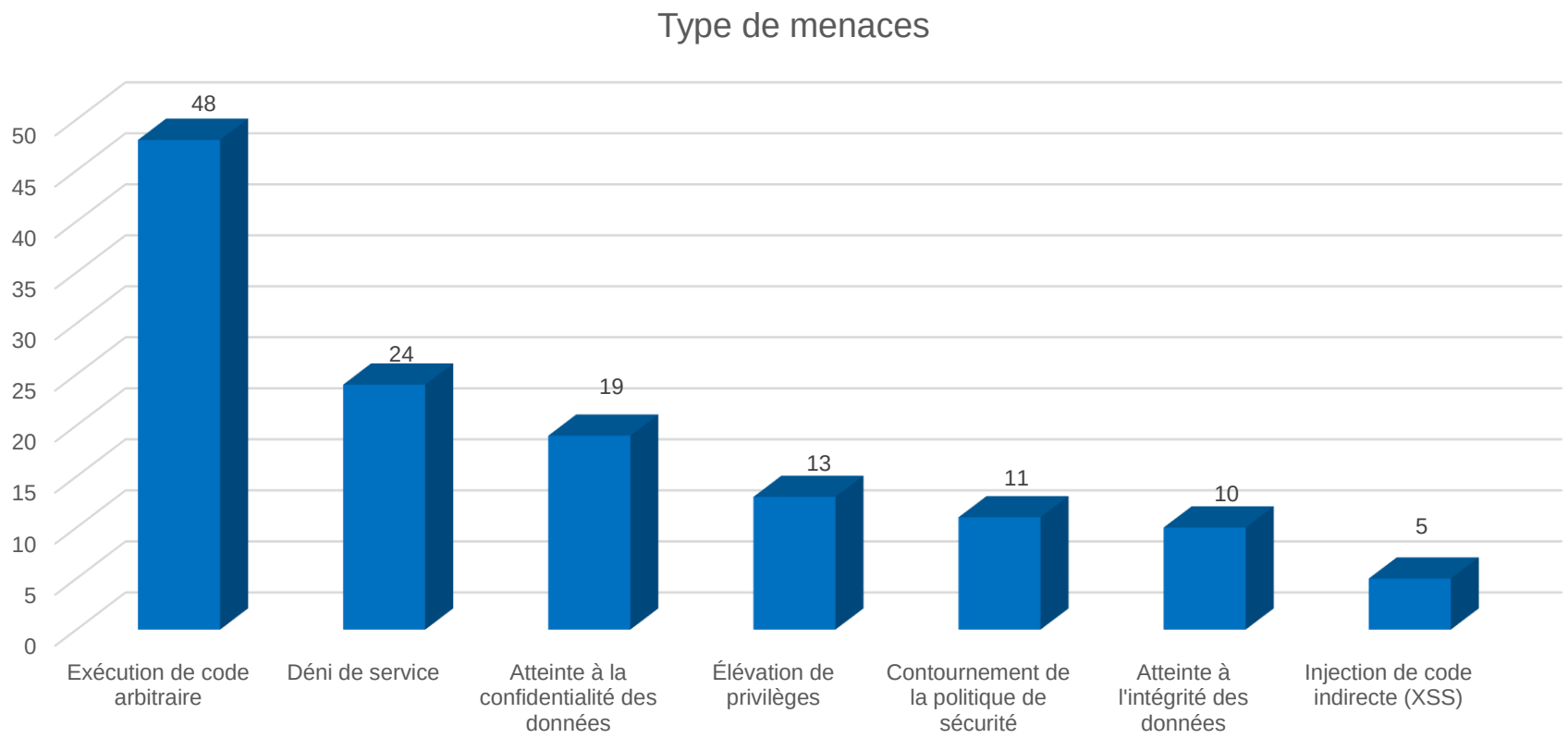
Types de solutions vulnérables

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

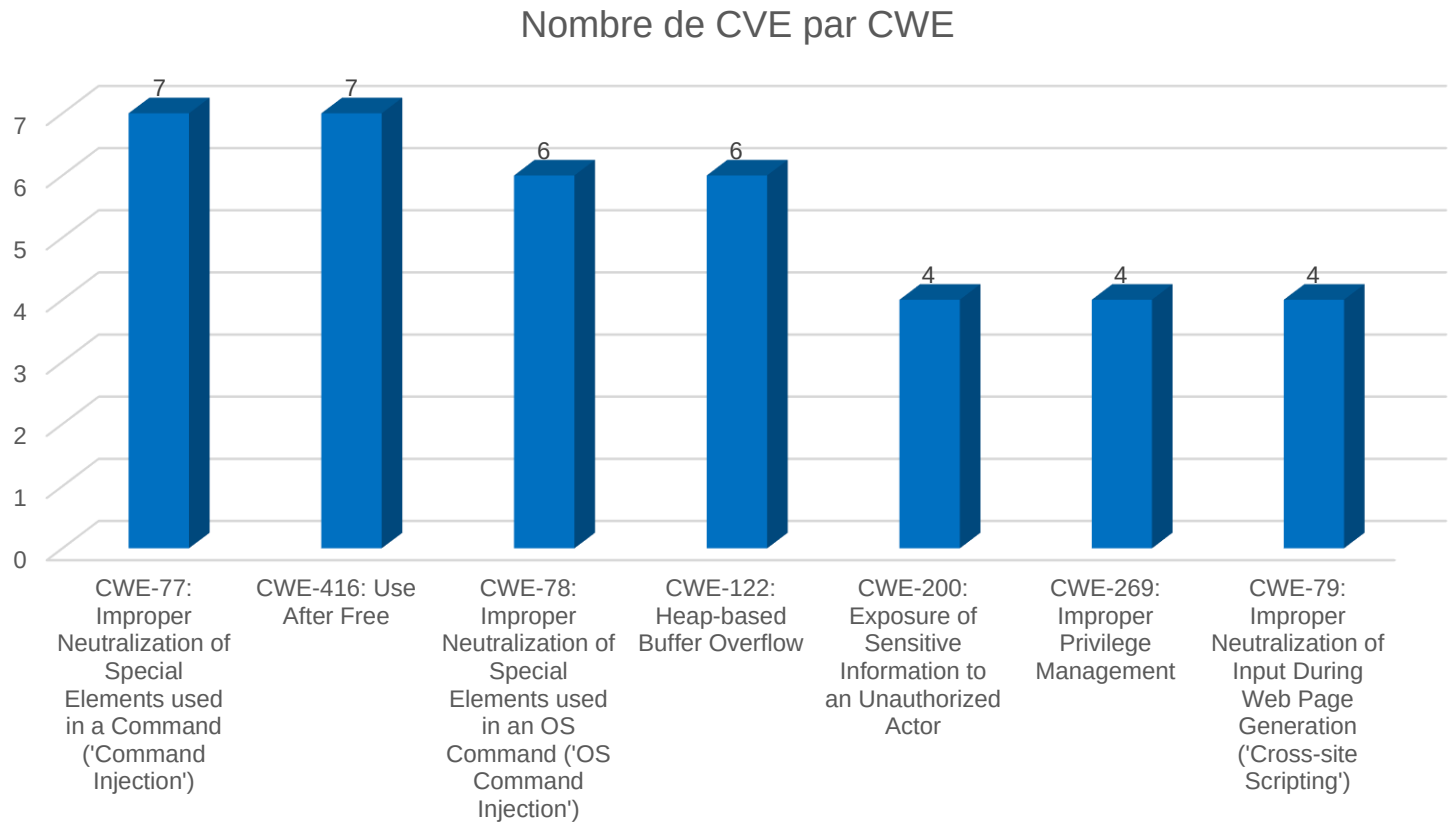
CVE par type de solution



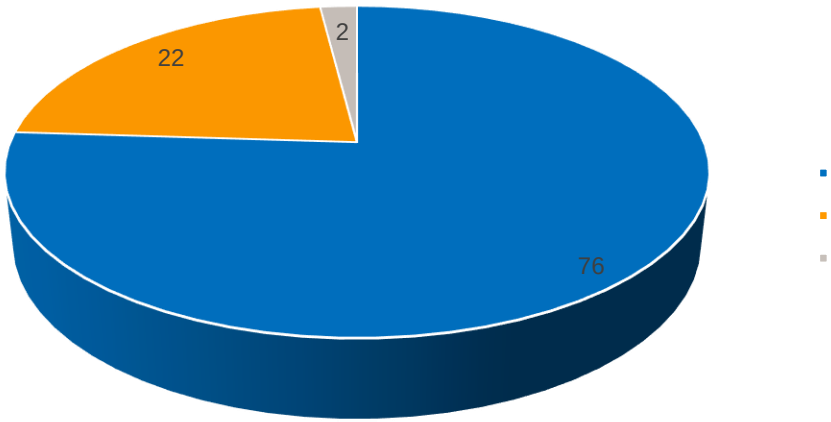
Types de menaces

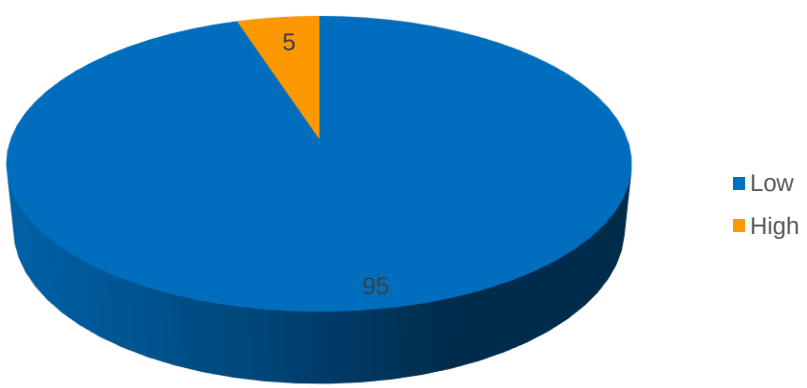


TOP 7 des failles selon le référentiel CWE



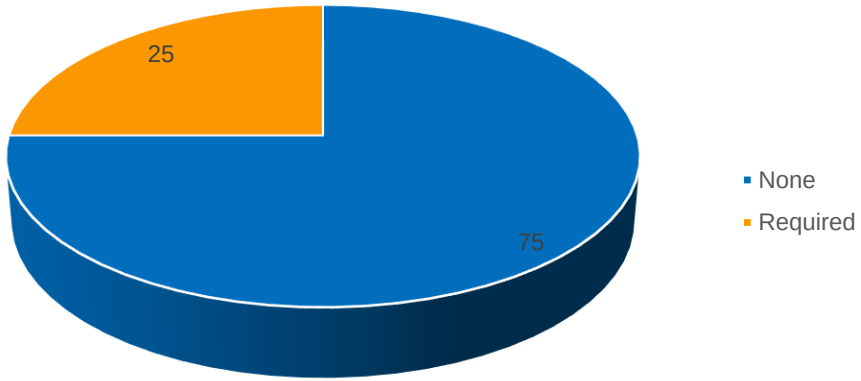
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



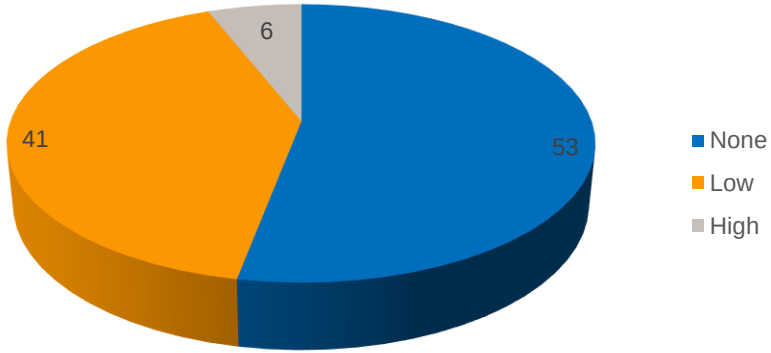


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

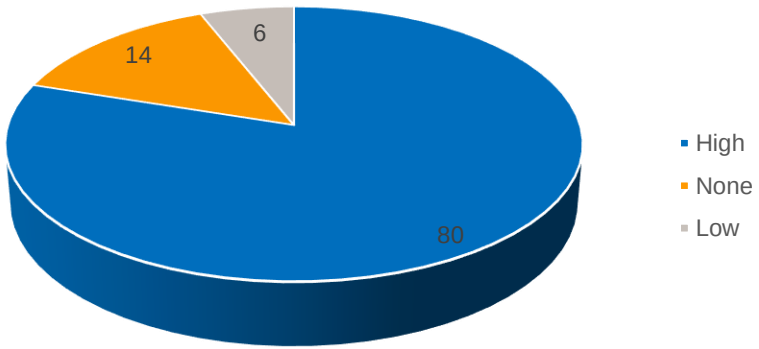


CVE par type de privilège requis

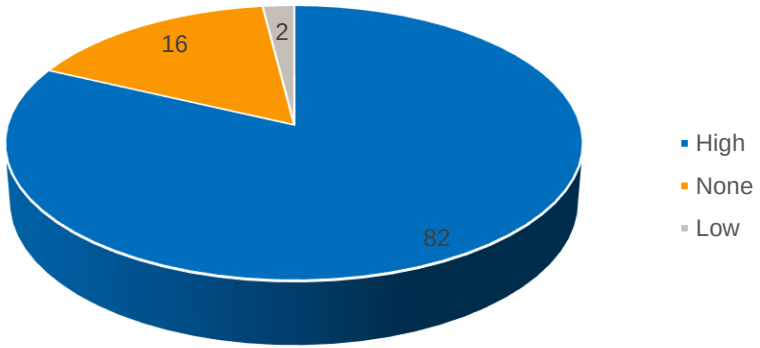


Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données

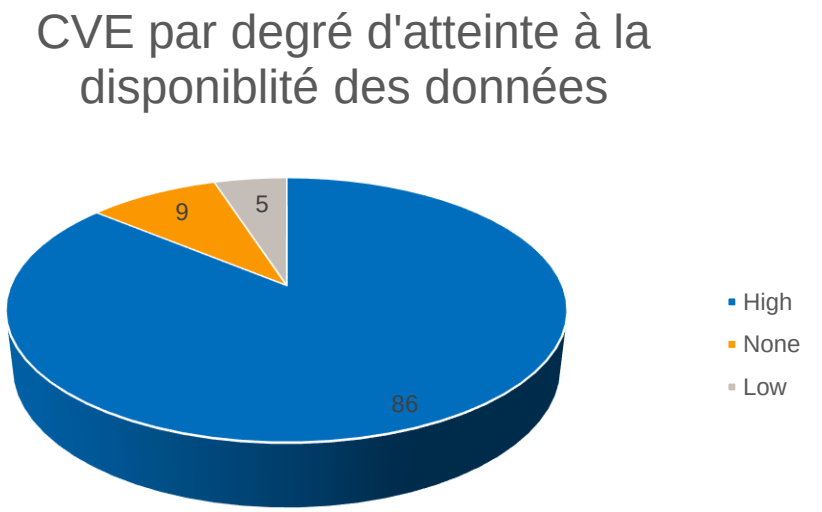
CVE par degré d'atteinte à l'intégrité des données

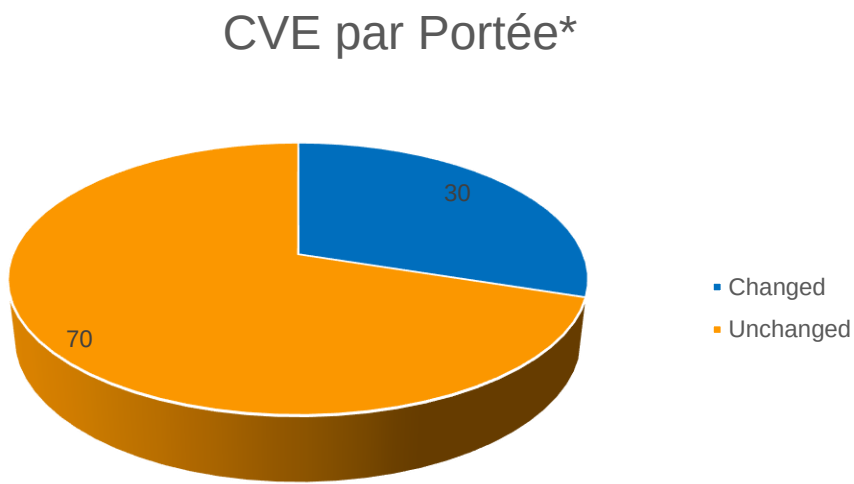


CVE par degré d'atteinte à la confidentialité des données



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.