AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

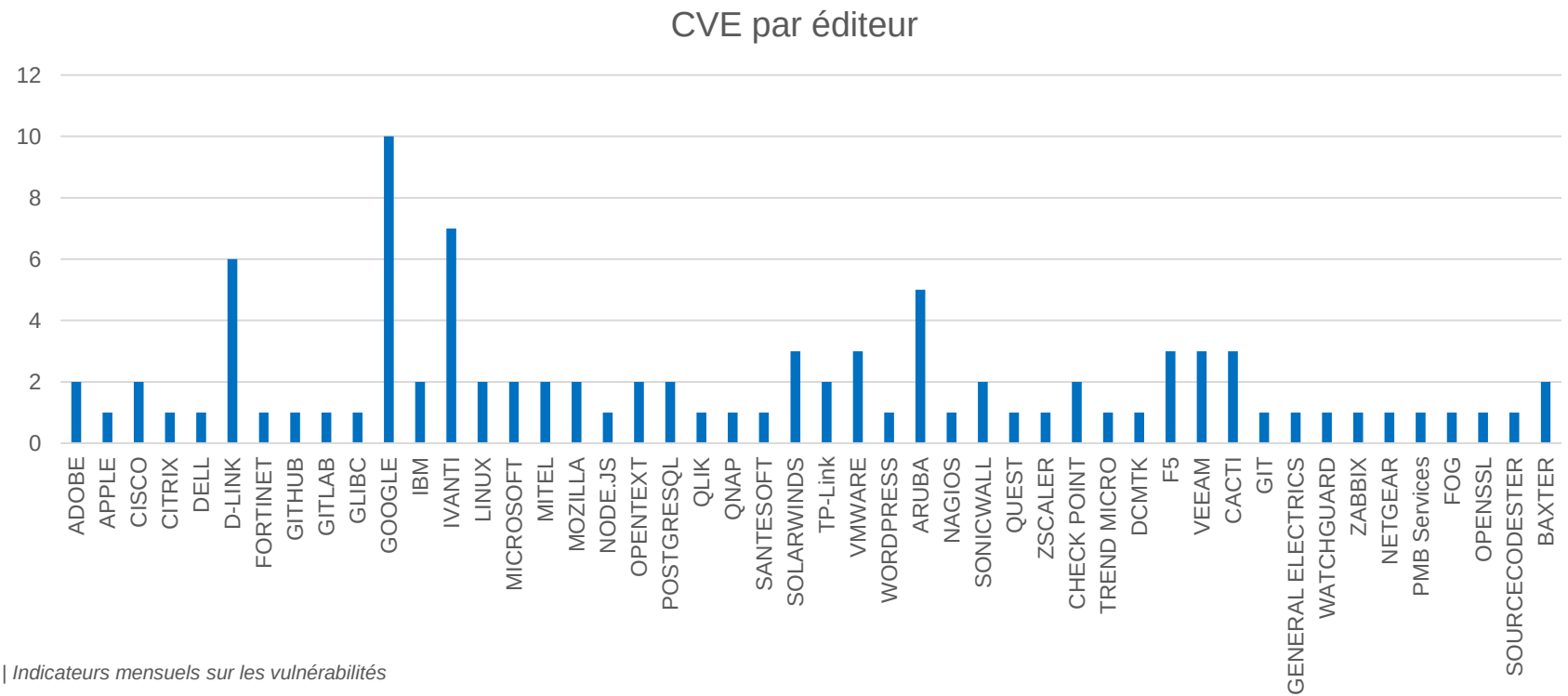
Indicateurs sur la publication des CVE pour le mois de mai 2024

CERT Santé

Juin 2024

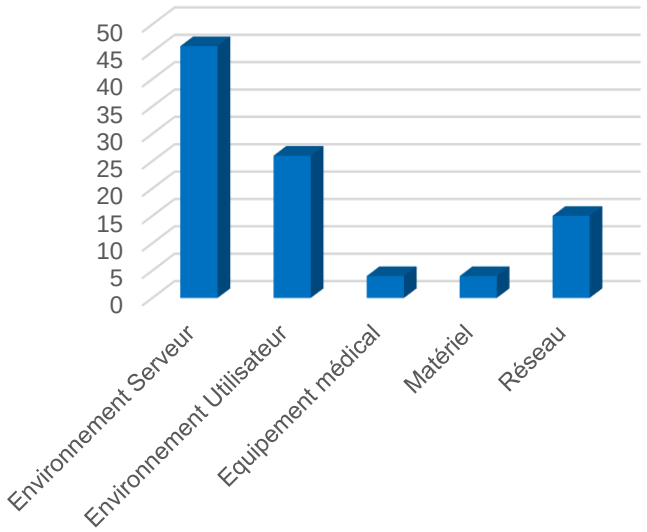
Nombre de CVE par éditeur

95 vulnérabilités ont été analysées et publiées (parmi lesquelles 7 alertes) sur le portail du CERT Santé.

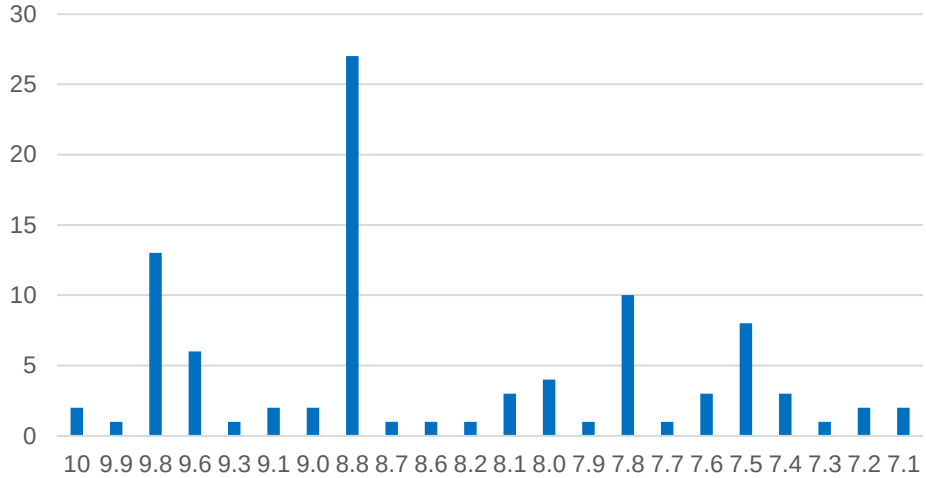


Nombre de CVE par catégorie de produit et score CVSS

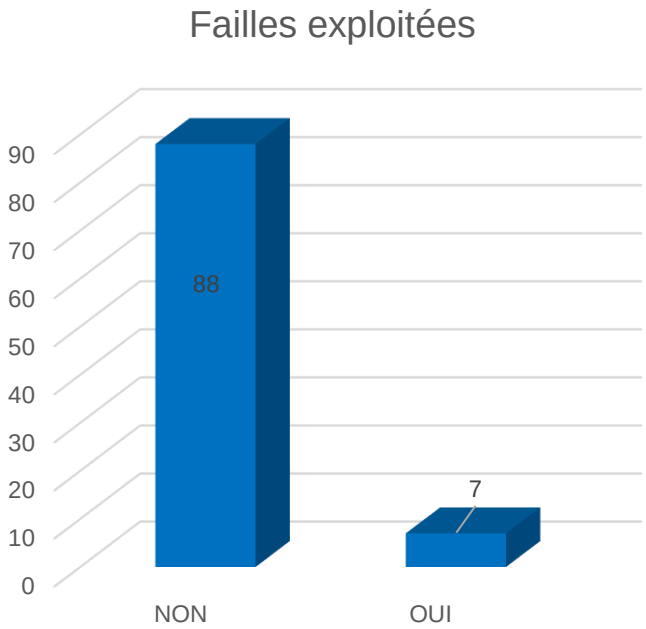
CVE par catégorie de solution

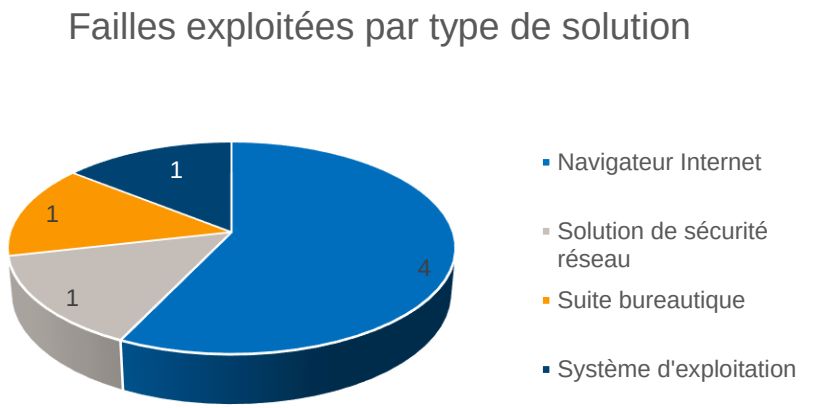


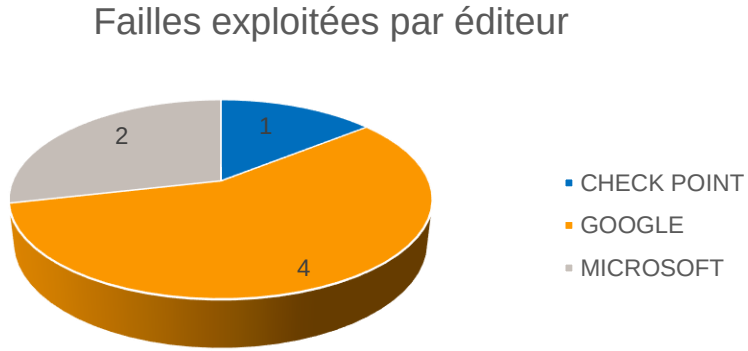
CVE par score CVSS



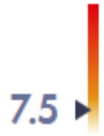
Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller



Check Point
(CVE-2024-24919)

Atteinte à la confidentialité

Exploitée

Une vulnérabilité dans l'accès VPN à distance de plusieurs passerelles de sécurité CheckPoint permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, de porter atteinte à la confidentialité des données.

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

Google Chrome
(CVE-2024-5274)

Exécution de code arbitraire

Exploitée

Une vulnérabilité de type « confusion de types » dans le moteur JavaScript V8 de Google Chrome permet à un attaquant non authentifié, en persuadant une victime de consulter un site Web spécifiquement forgé, d'exécuter du code arbitraire.

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

Microsoft
(CVE-2024-30051)

Élévation de privilèges

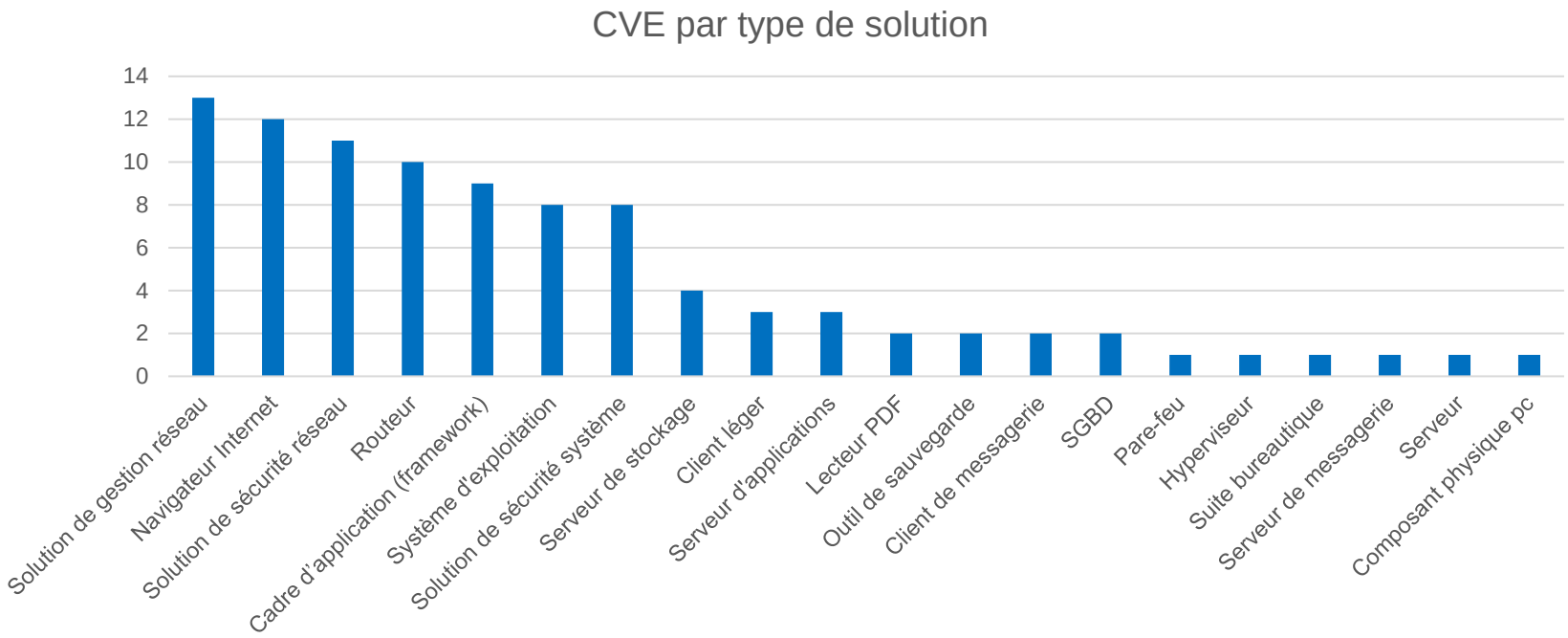
Exploitée

Un défaut de gestion de la mémoire dans la bibliothèque DWM Core de Windows permet à un attaquant authentifié, en envoyant des requêtes spécifiquement forgées, d'élever ses privilèges vers des droits SYSTEM.

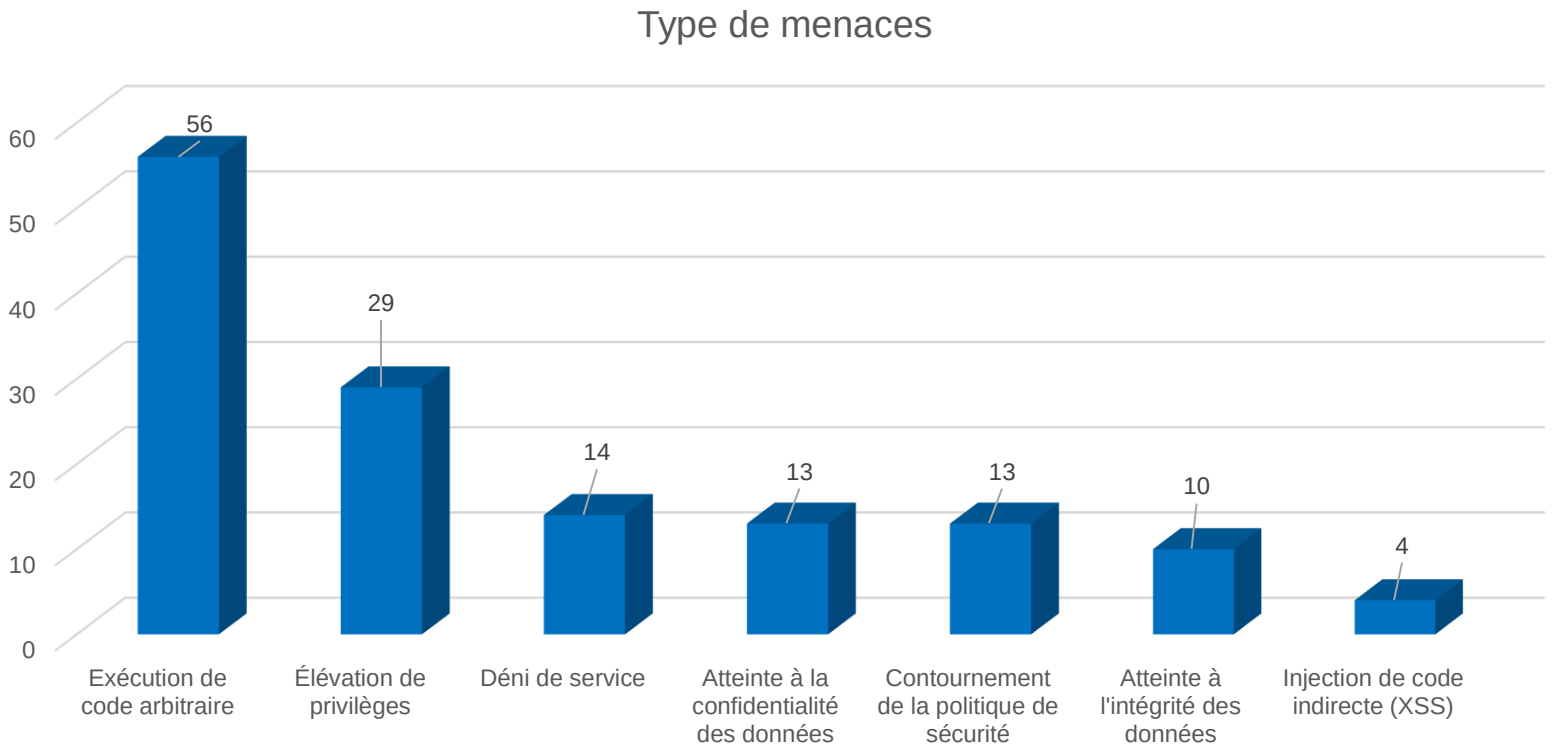
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

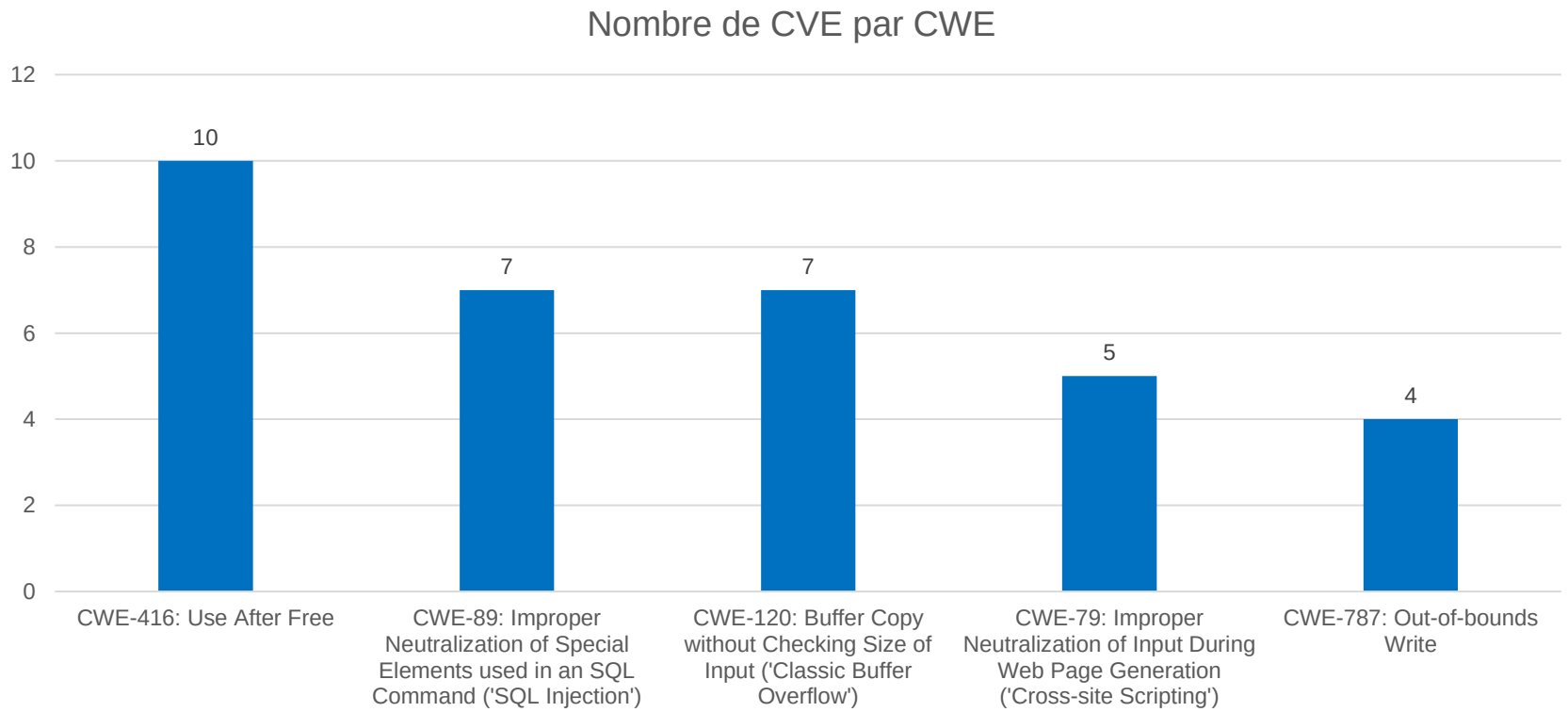
Les solutions de gestion réseau, les navigateurs internet et les solutions de sécurité réseau sont les principaux types d'équipements affectés par les vulnérabilités publiées.



Types de menaces

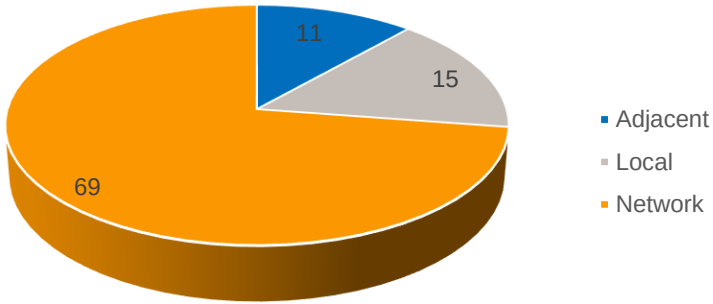


TOP 5 des failles selon le référentiel CWE

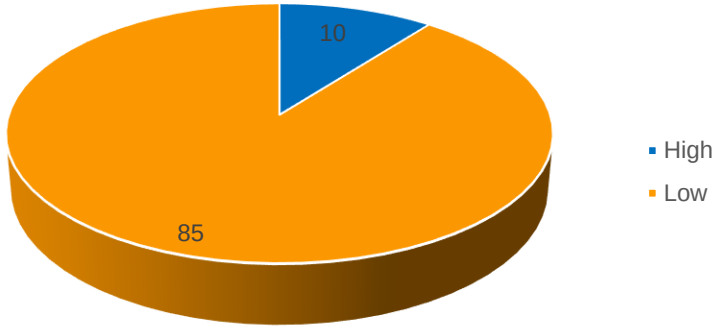


Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque

CVE par type de vecteur d'attaque

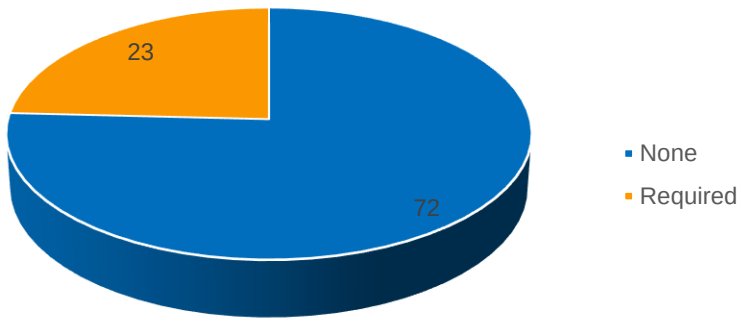


CVE par complexité d'attaque

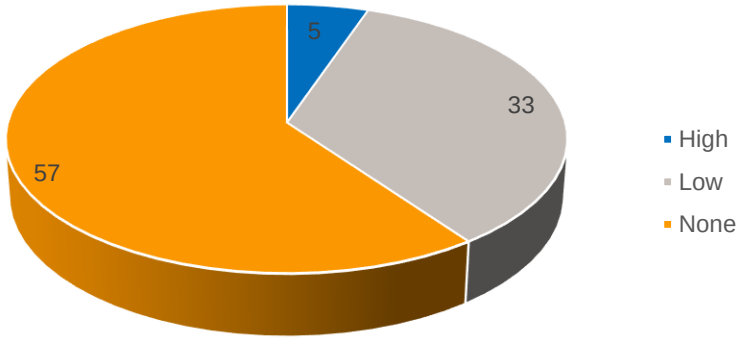


Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

CVE par interaction utilisateur

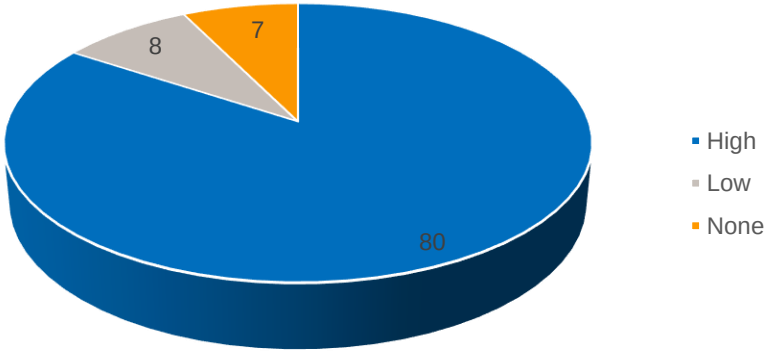


CVE par type de privilèges requis

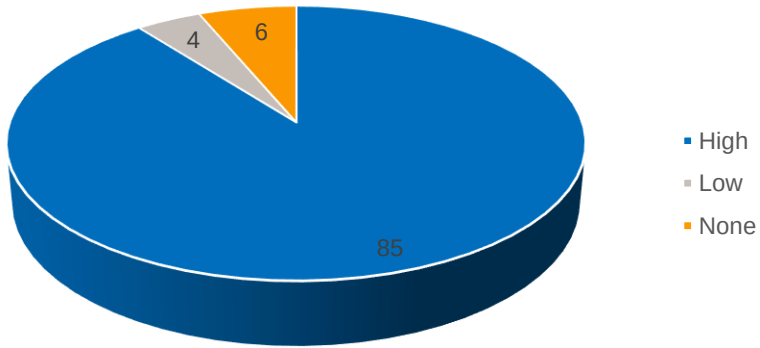


Nombre de CVE selon l’impact sur l’intégrité et sur la confidentialité des données

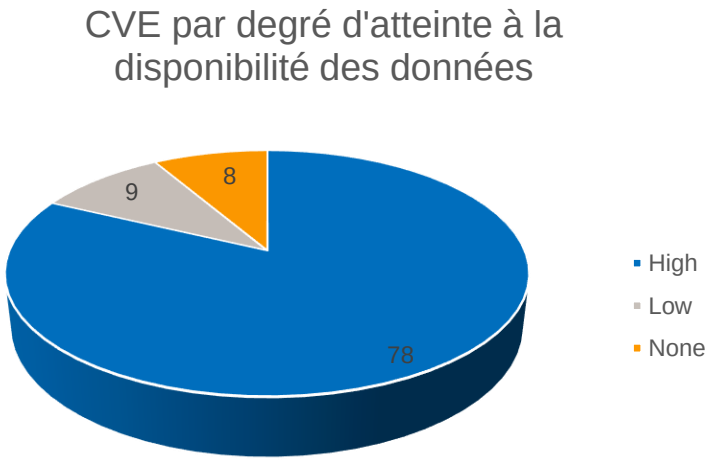
CVE par degré d'atteinte à l'intégrité des données

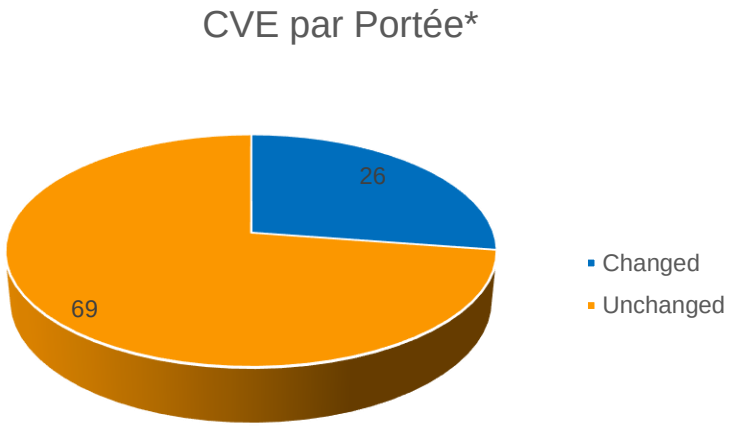


CVE par degré d'atteinte à la confidentialité des données



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.