AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

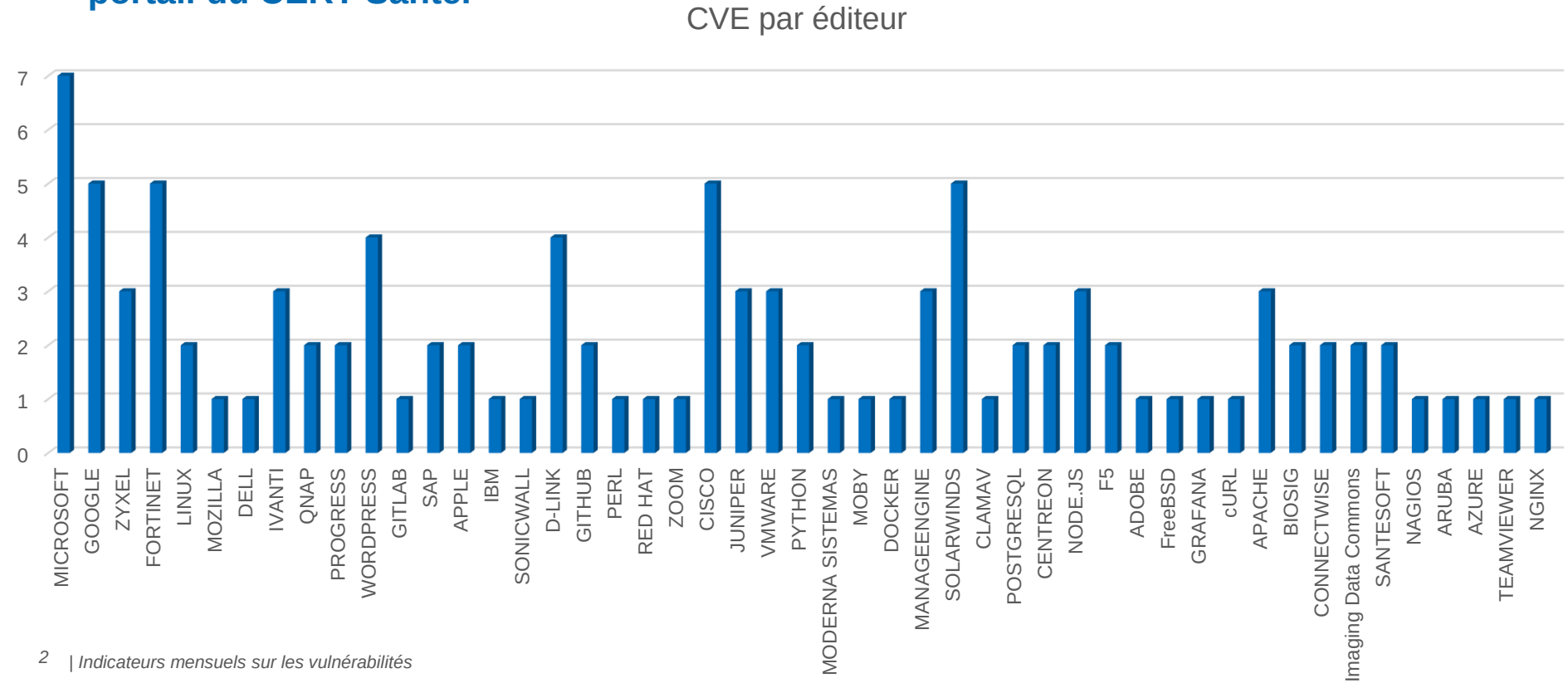
Indicateurs sur la publication des CVE pour le mois de mars 2024

CERT Santé

avril 2024

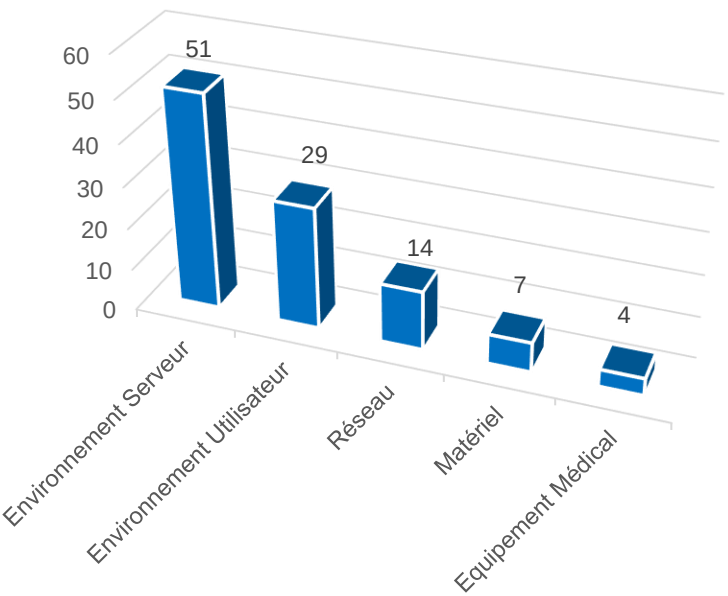
Nombre de CVE par éditeur

105 vulnérabilités ont été analysées et publiées (parmi lesquelles 4 alertes) sur le portail du CERT Santé.

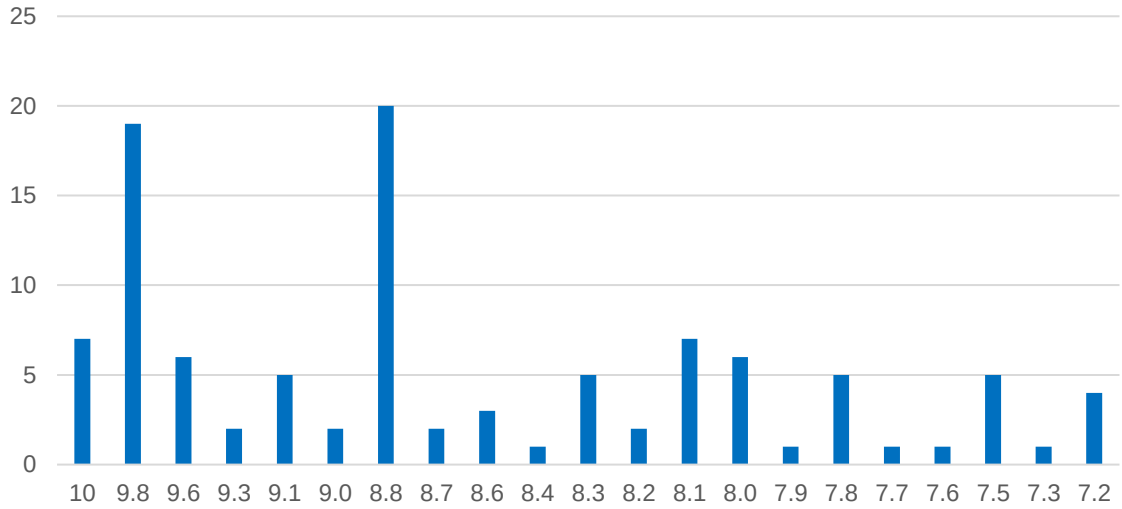


Nombre de CVE par catégorie de produit et score CVSS

CVE par catégorie de solution

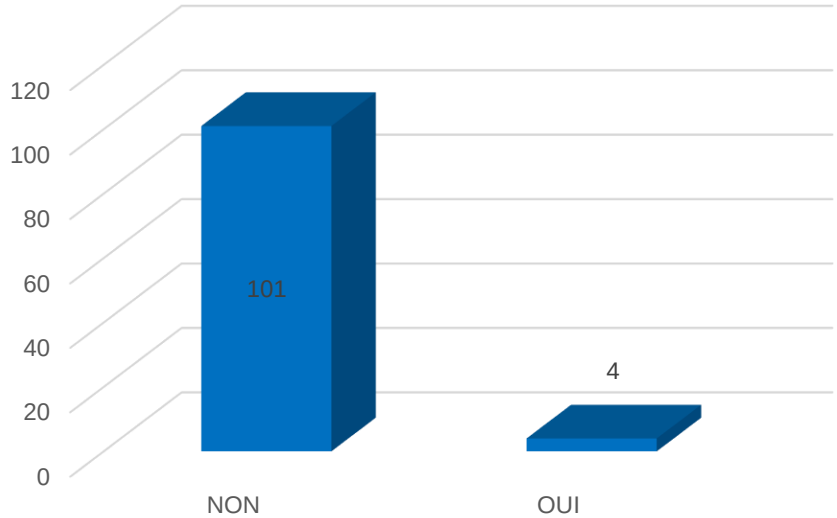


CVE par score CVSS

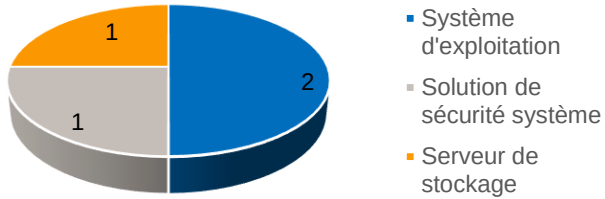


Vulnérabilités exploitées

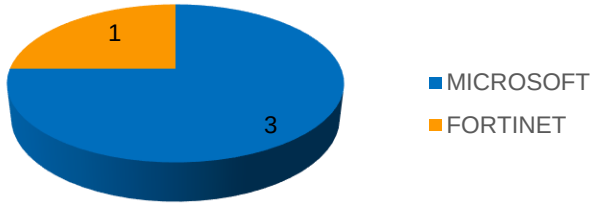
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

Fortinet
(CVE-2023-48788)

Exécution de code arbitraire

Exploitée

Une vulnérabilité de type « injection SQL » dans FortiClientEMS 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.

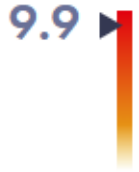
Microsoft
(CVE-2023-29360)

Élévation de privilèges

Exploitée

Un défaut dans le pilote mskssrv de Microsoft permet à un attaquant, en exécutant un programme, d'obtenir les privilèges SYSTEM.

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



Ivanti
(CVE-2023-46808)

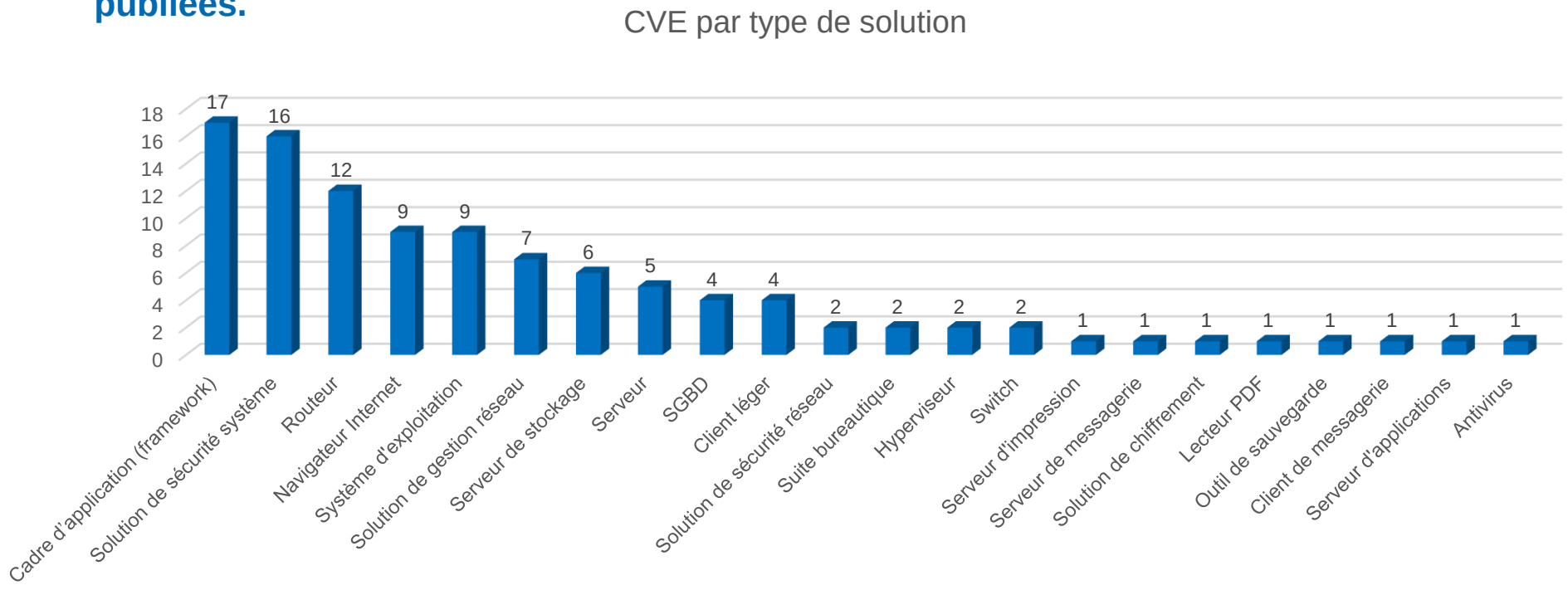
Exécution de code arbitraire

Une vulnérabilité d'écriture de fichiers dans Ivanti Neurons pour ITSM permet à un attaquant authentifié, en écrivant des fichiers spécifiquement forgés dans des répertoires sensibles, d'exécuter du code arbitraire.

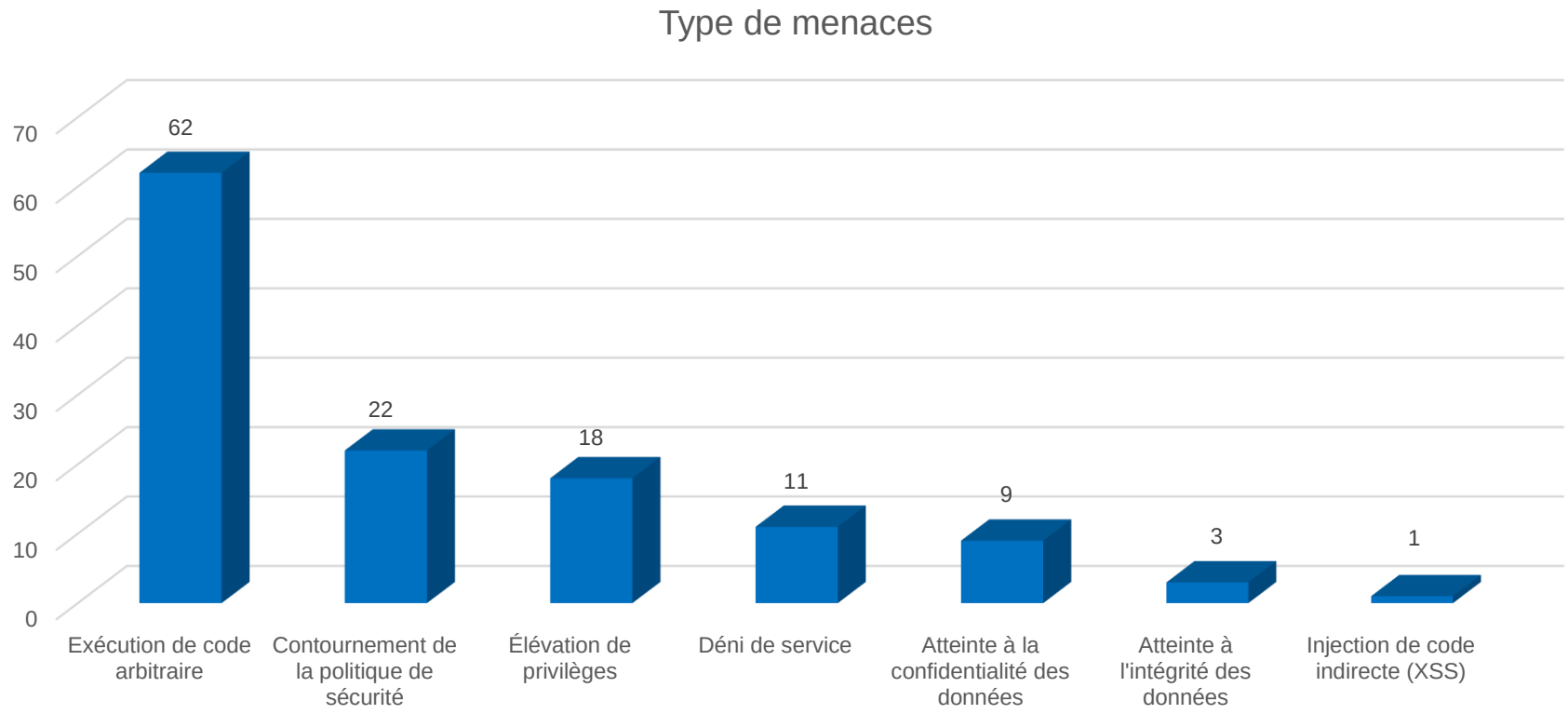
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

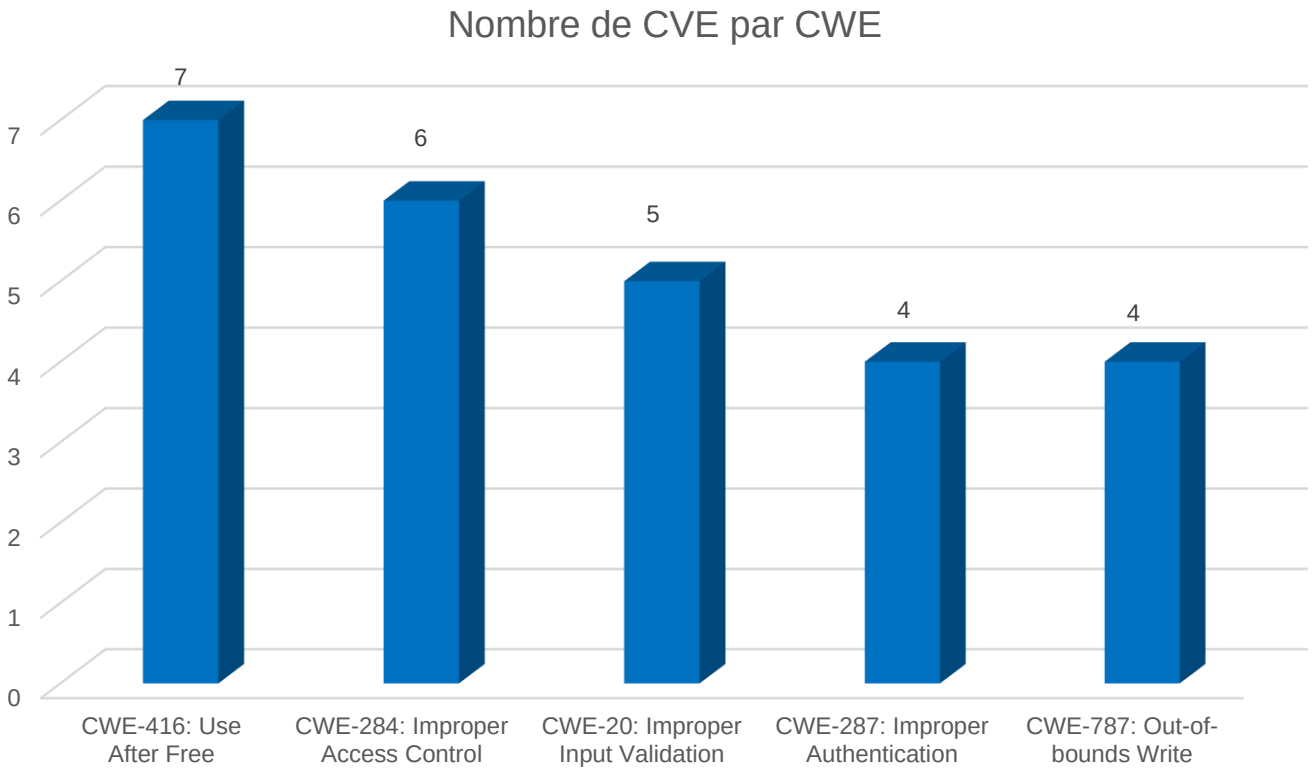
Les cadres d'application (framework), les solutions de sécurité système et les routeurs sont les principaux types d'équipements affectés par les vulnérabilités publiées.



Types de menaces

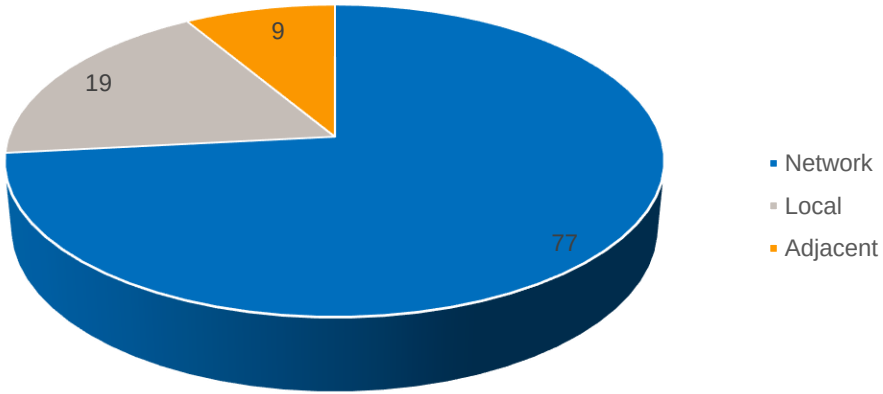


TOP 5 des failles selon le référentiel CWE

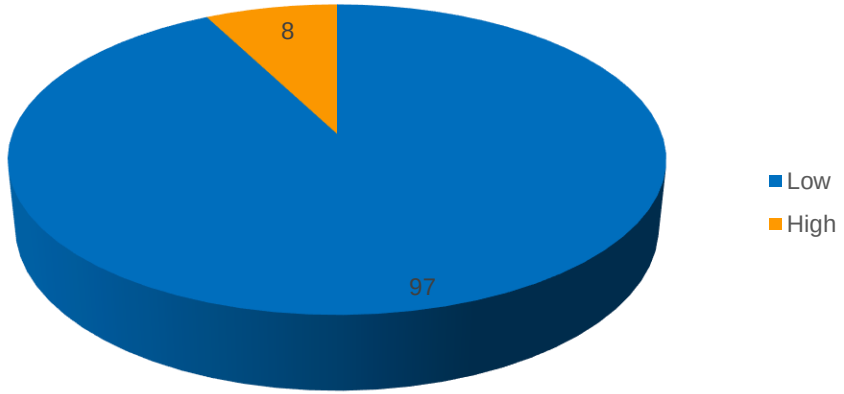


Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque

CVE par type de vecteur d'attaque

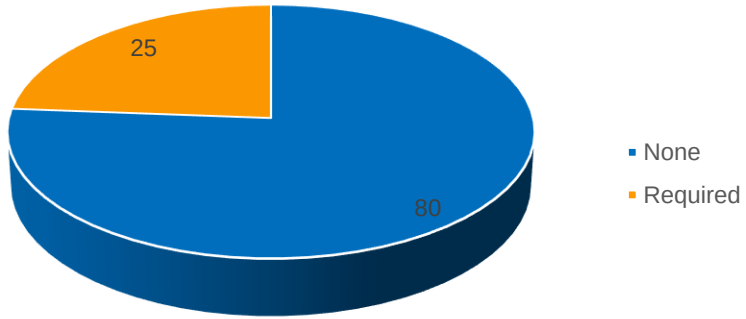


CVE par complexité d'attaque

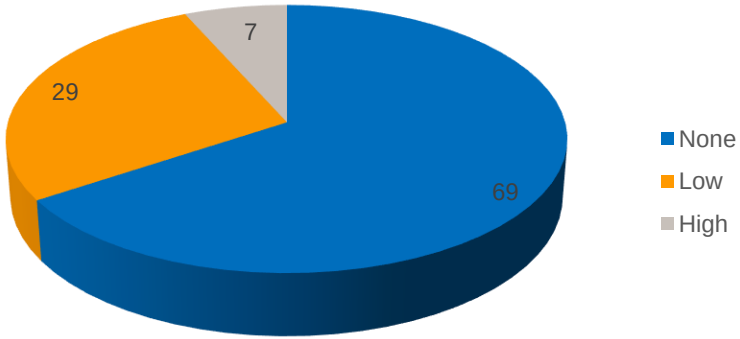


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

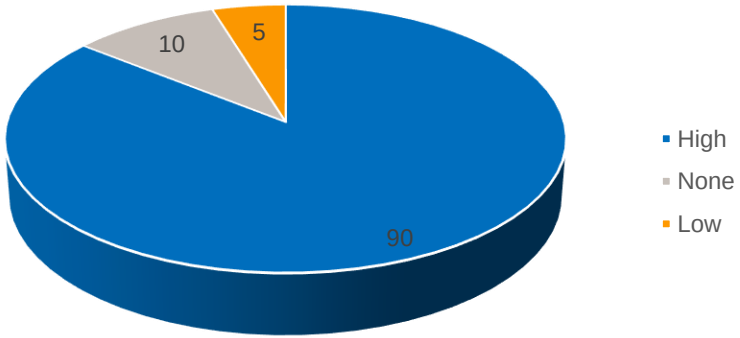


CVE par type de privilège requis

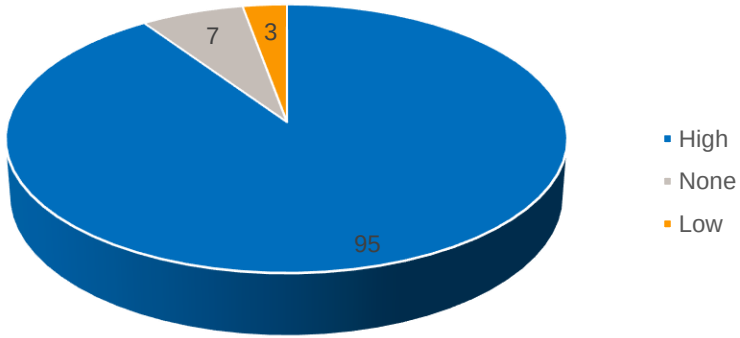


Nombre de CVE selon l’impact sur l’intégrité et sur la confidentialité des données

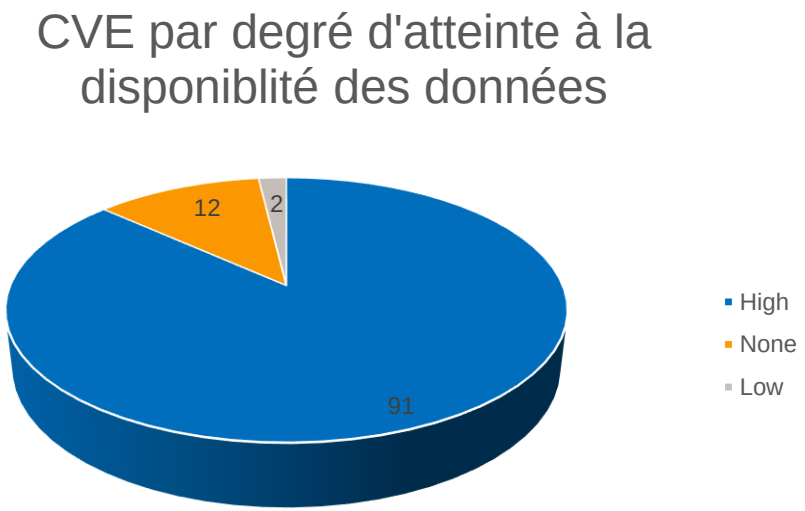
CVE par degré d'atteinte à l'intégrité des données

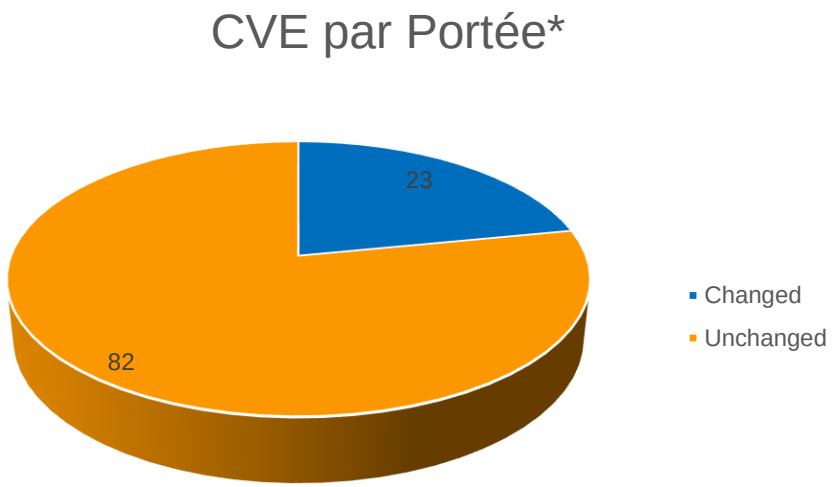


CVE par degré d'atteinte à la confidentialité des données



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.