AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

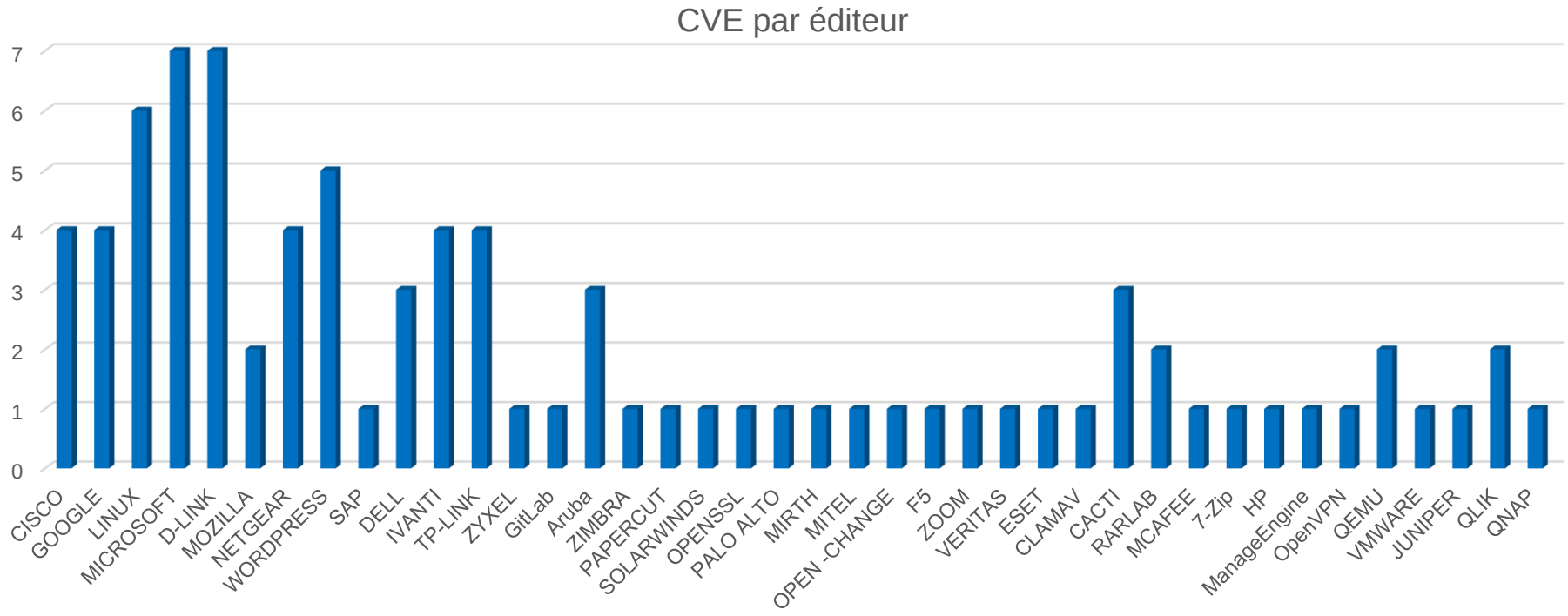
Indicateurs sur la publication des CVE pour le mois de août 2023

CERT Santé

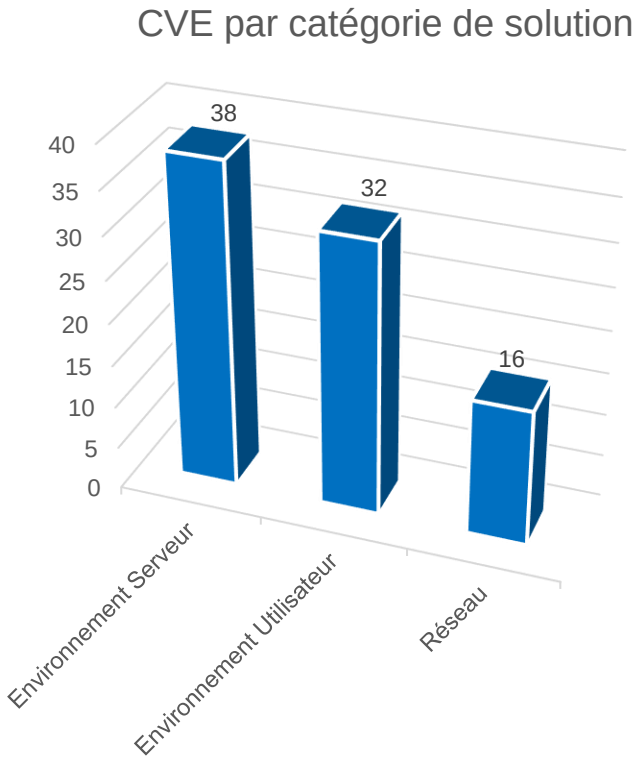
Septembre 2023

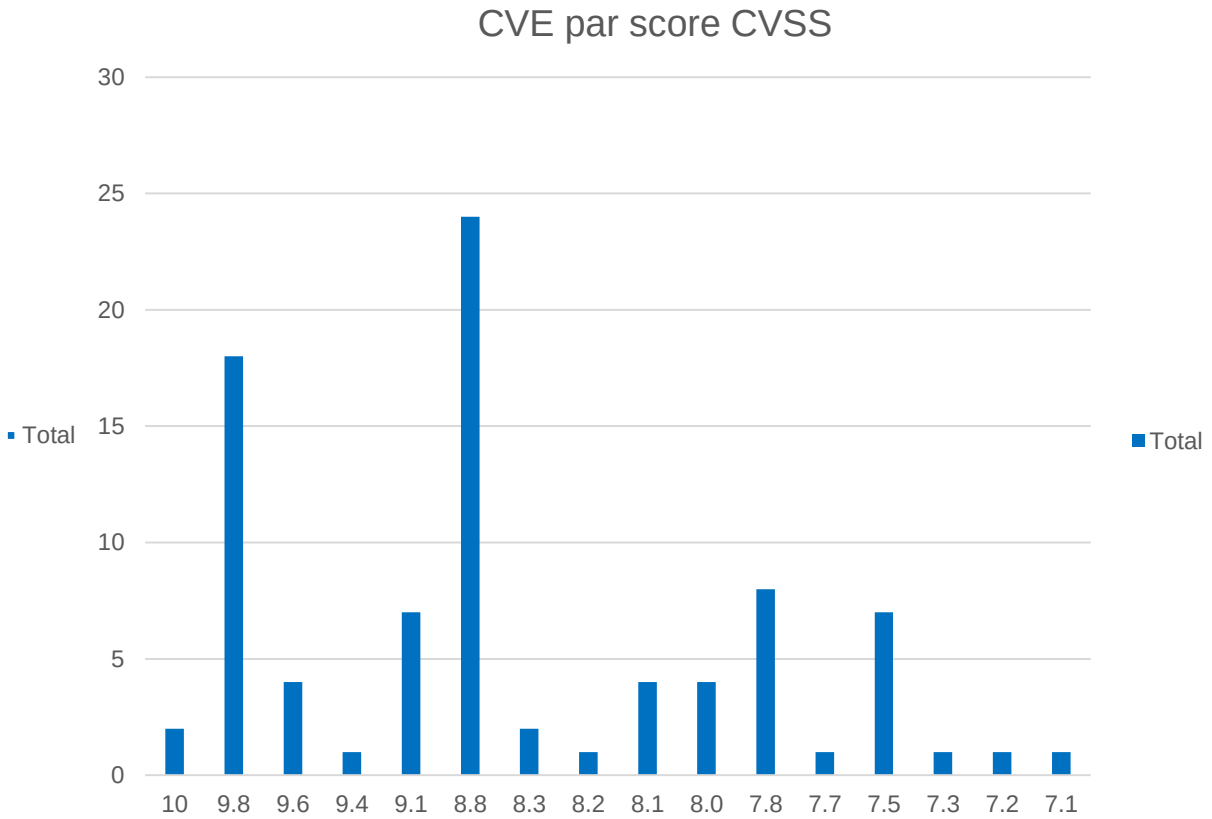
Nombre de CVE par éditeur

86 vulnérabilités ont été analysées et publiées sur le portail du CERT Santé.



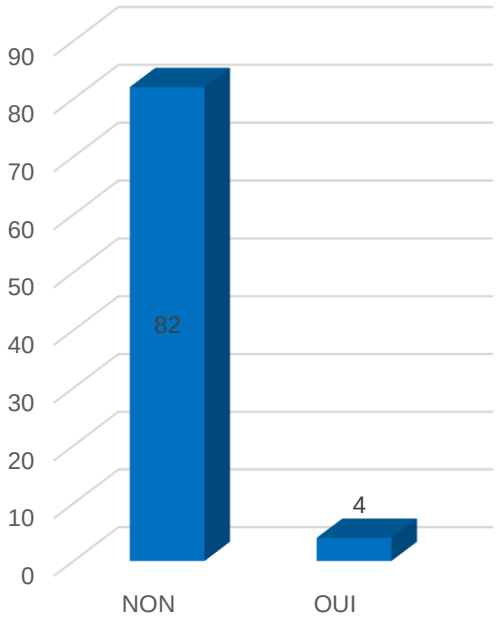
Nombre de CVE par catégorie de produit et score CVSS



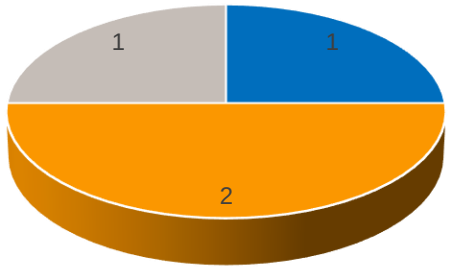


Vulnérabilités exploitées

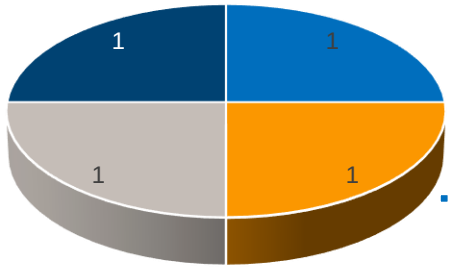
Failles exploitées



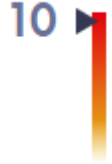
Failles exploitées par éditeur



Failles exploitées par type de solution



Les vulnérabilités critiques à surveiller



Ivanti Endpoint Manager Mobile
(CVE-2023-35082)

Contournement de la politique de sécurité

Exploitée

Un attaquant non authentifié peut accéder à l'interface de programmation de l'application, obtenir des informations sensibles ou effectuer des modifications sur la plateforme.

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

RARLAB WinRAR
(CVE-2023-38831)

Exécution de code arbitraire

Exploitée

Un attaquant non authentifié peut exécuter du code arbitraire sur le système de la victime si elle ouvre une archive spécifiquement forgée .

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

Ivanti Sentry
(CVE-2023-38035)

Exécution de code arbitraire

Exploitée

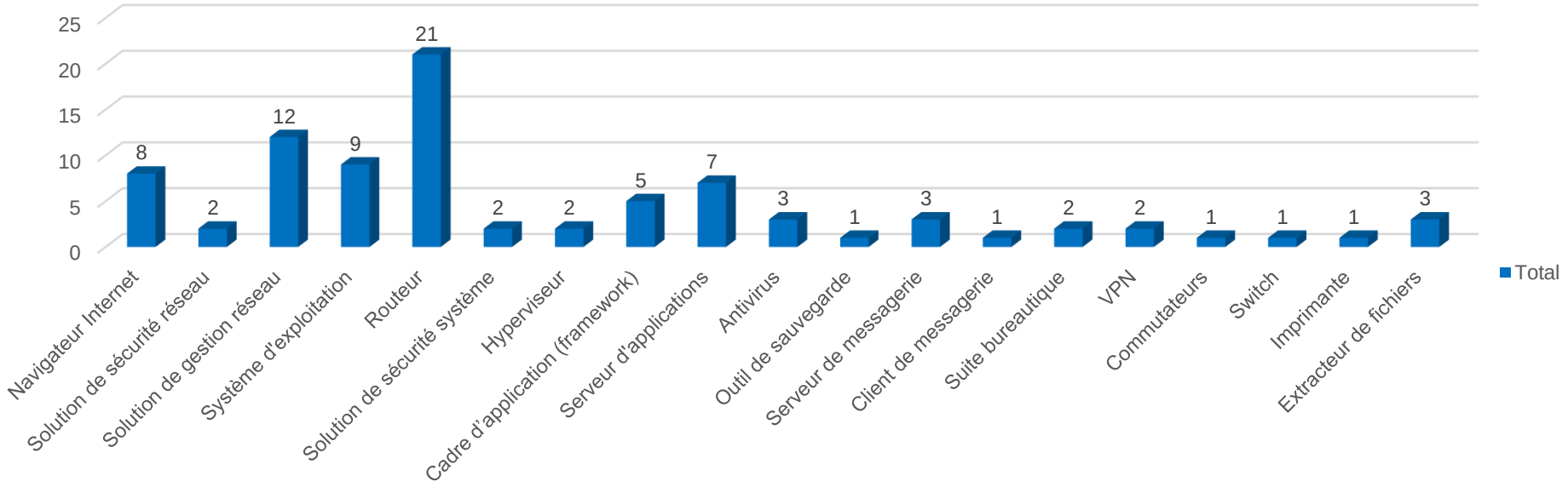
Un attaquant non authentifié peut contourner la politique de sécurité et exécuter du code sur le système avec les privilèges root.

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

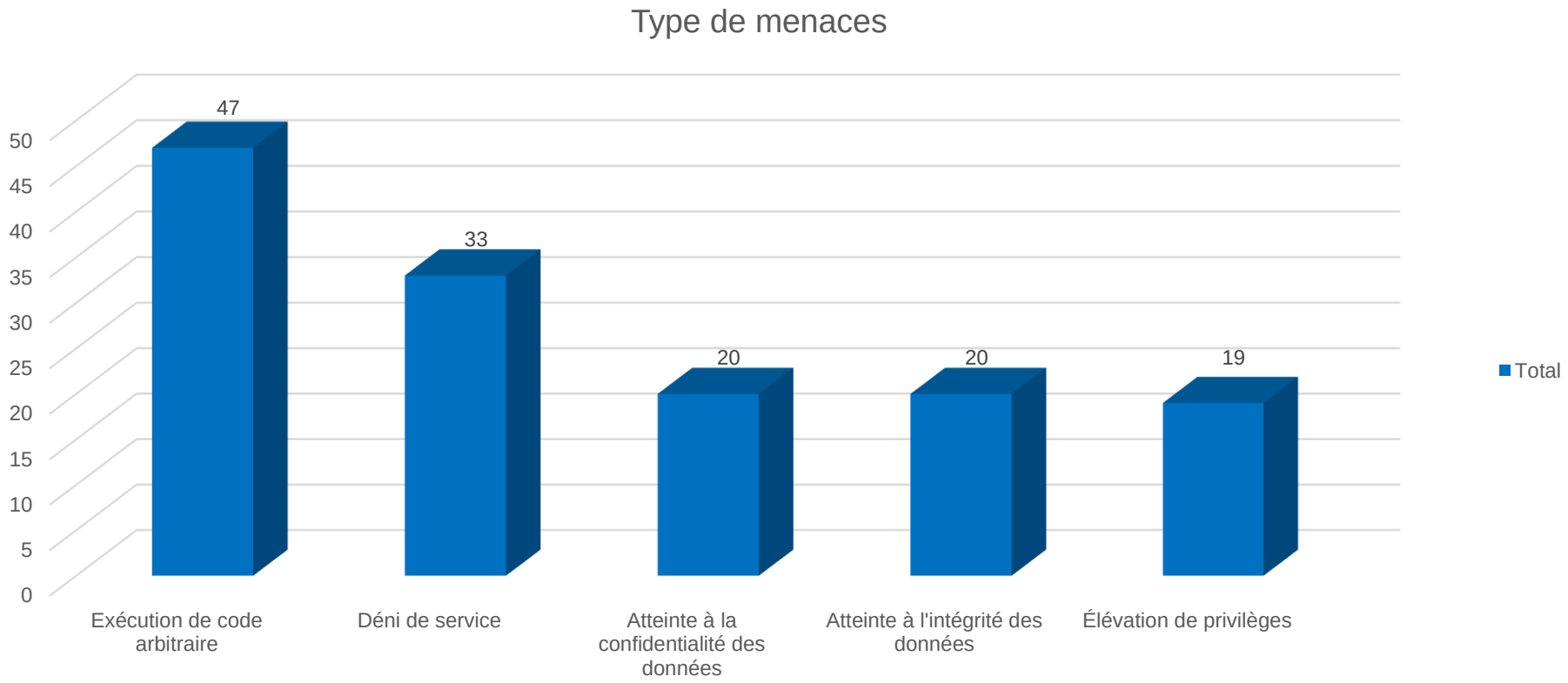
Types de solution vulnérables

Les routeurs, les solutions de gestion réseau et les systèmes d'exploitation sont les principaux types d'équipements affectés par les vulnérabilités publiées.

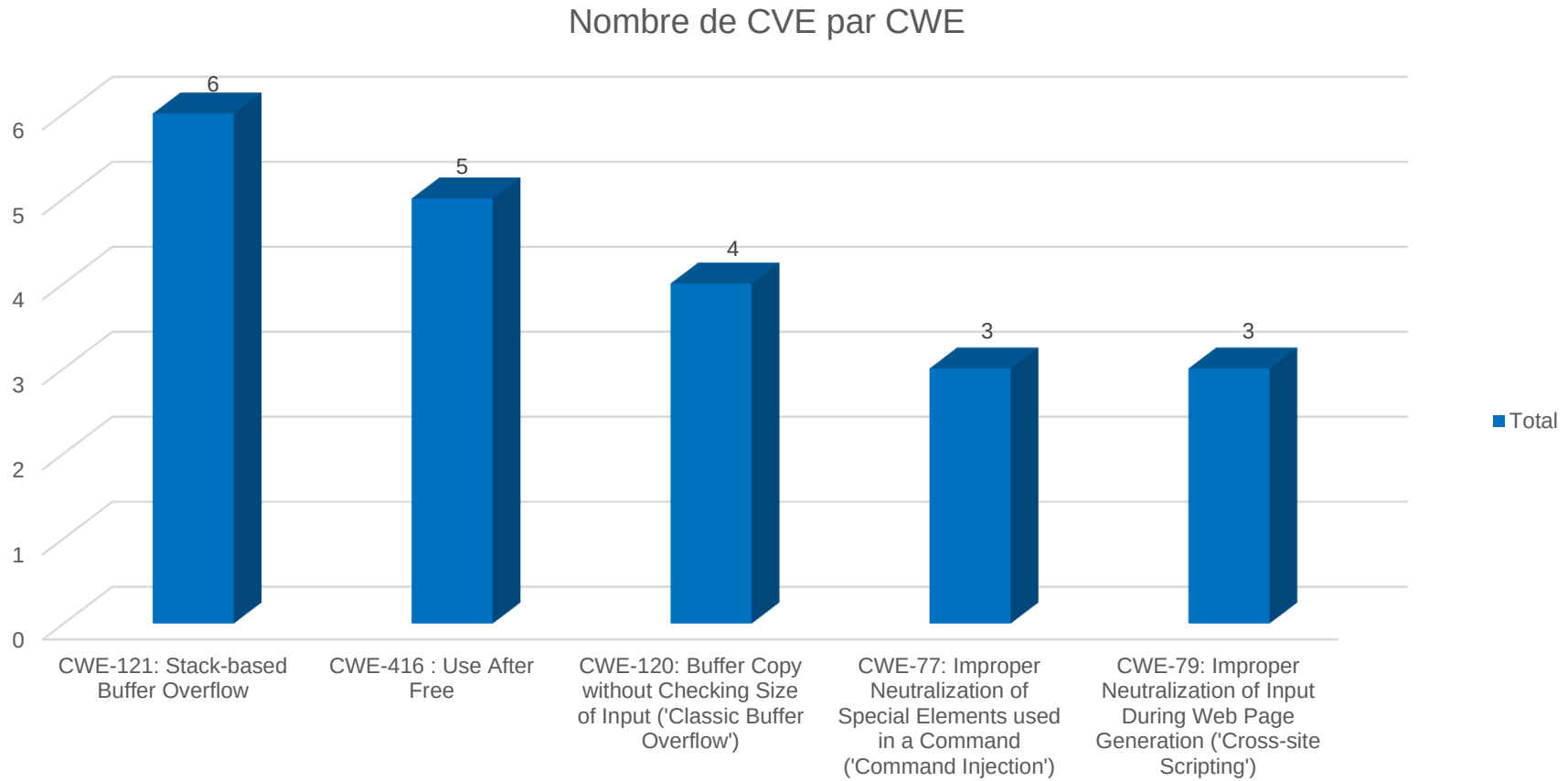
CVE par type de solution



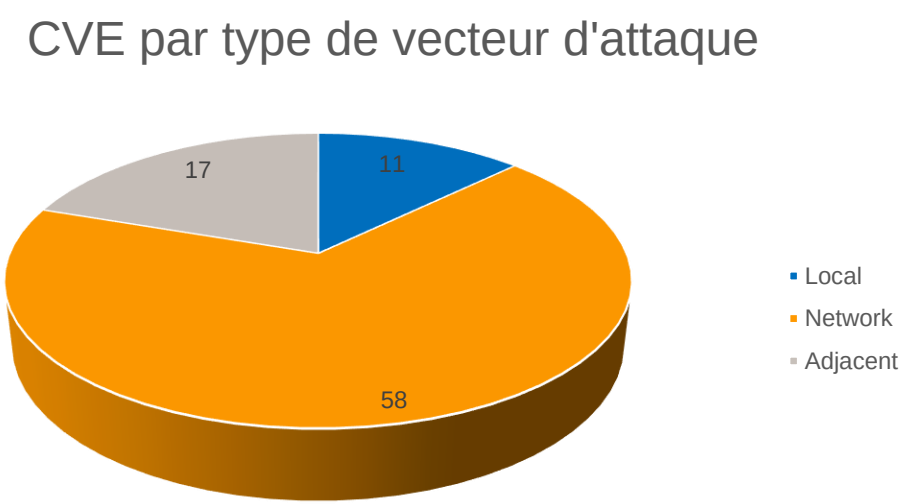
Types de menaces

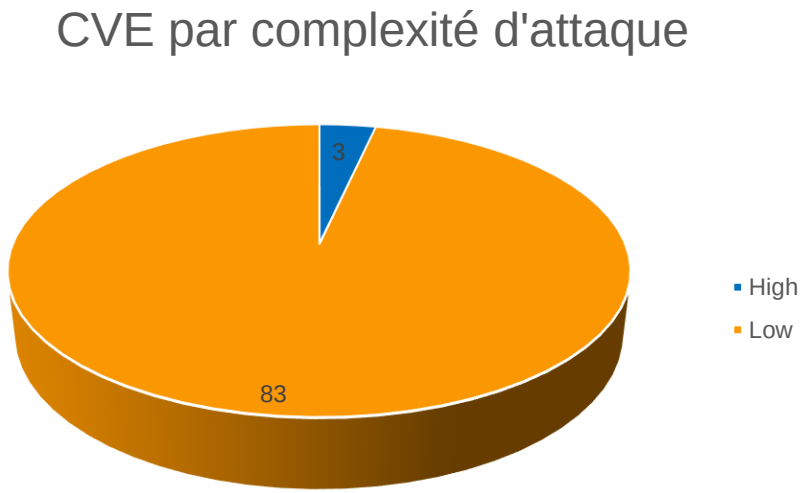


TOP 5 des failles selon le référentiel CWE



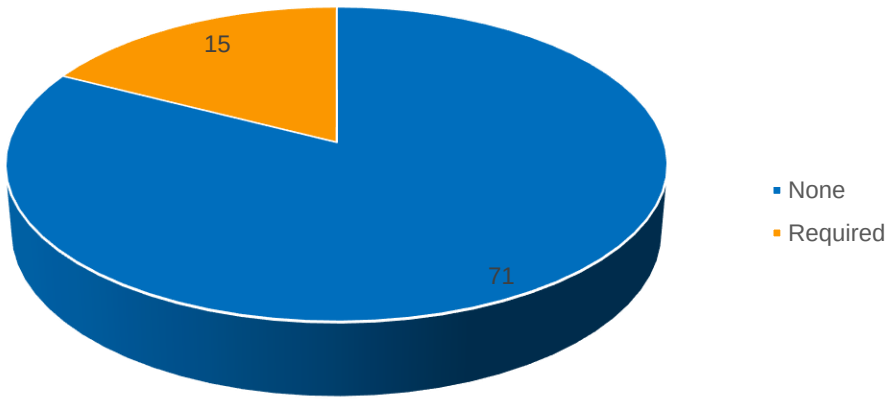
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



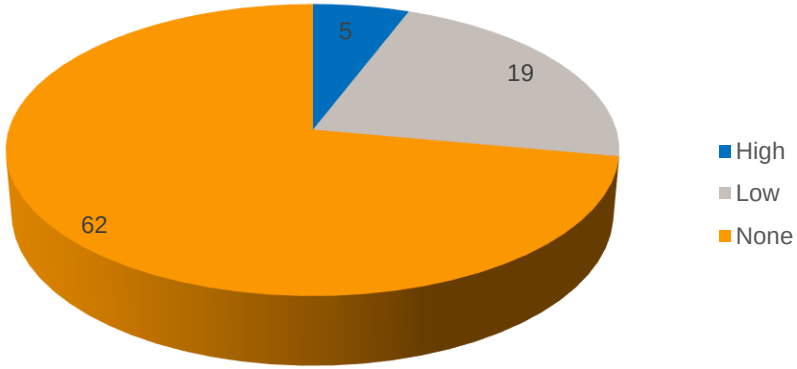


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

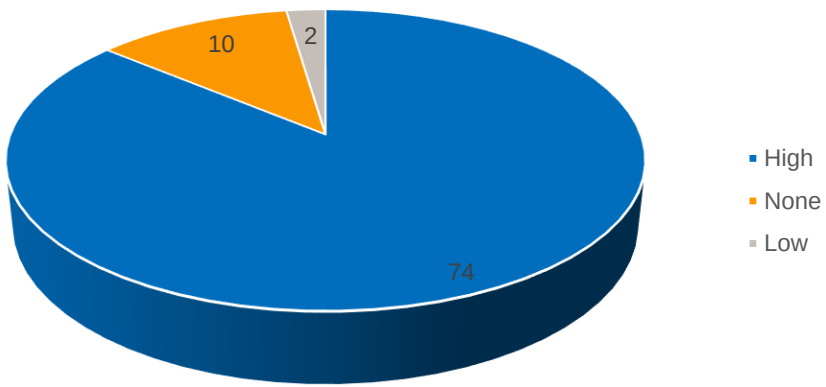


CVE par type de privilège requis

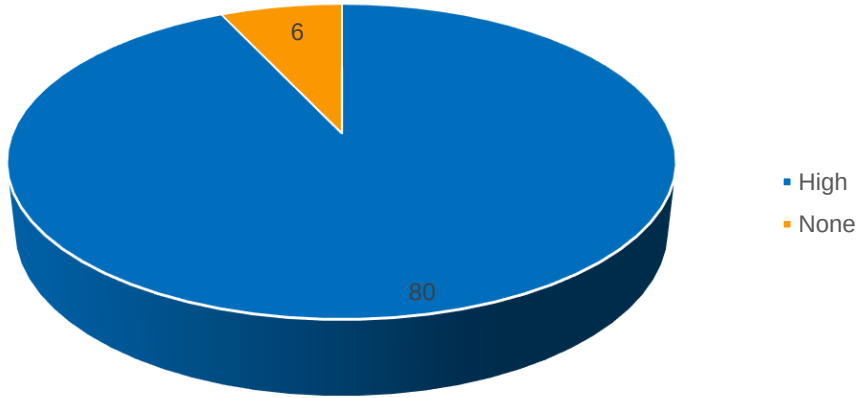


Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données

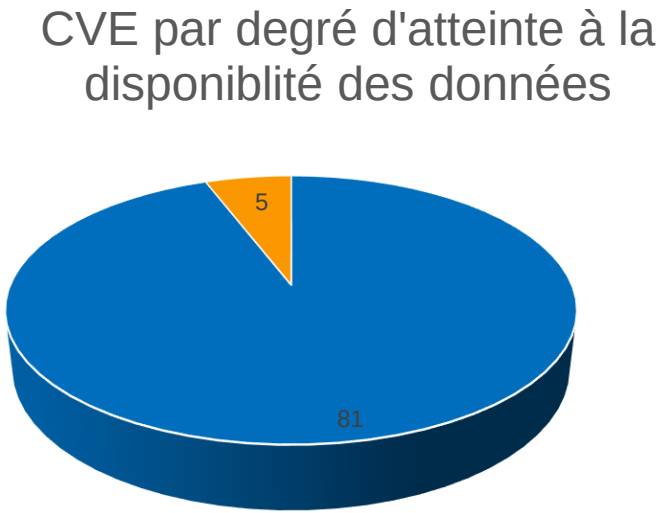
CVE par degré d'atteinte à l'intégrité des données

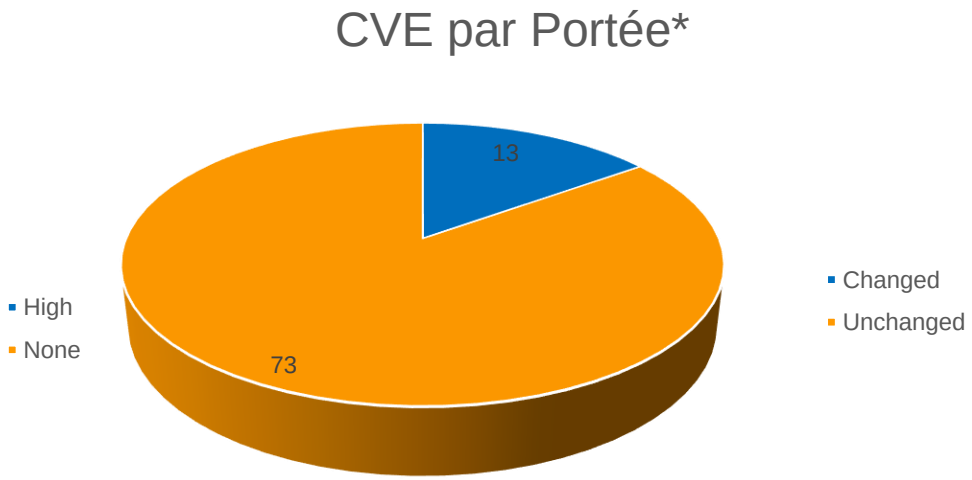


CVE par degré d'atteinte à la confidentialité des données



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.