AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

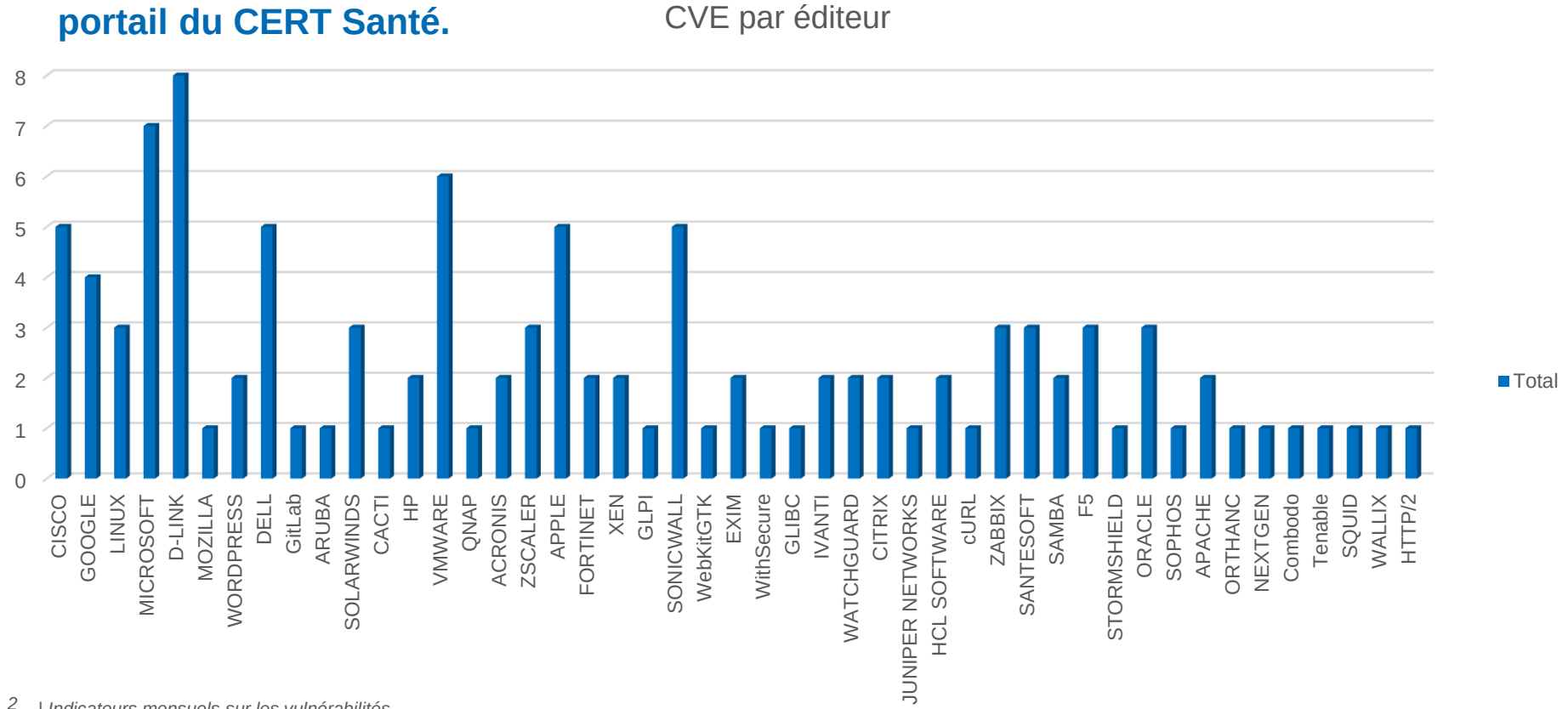
Indicateurs sur la publication des CVE pour le mois d'octobre 2023

CERT Santé

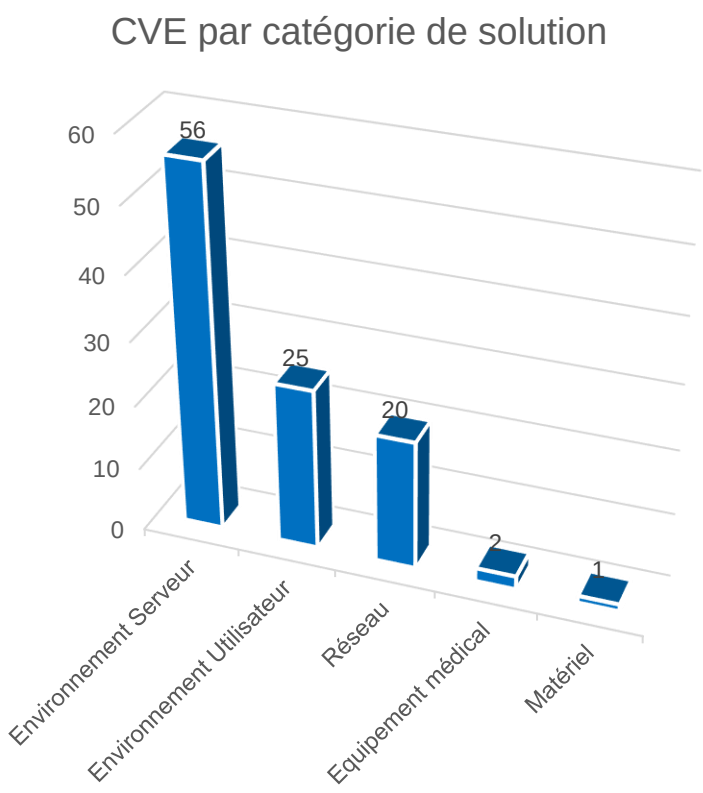
Novembre 2023

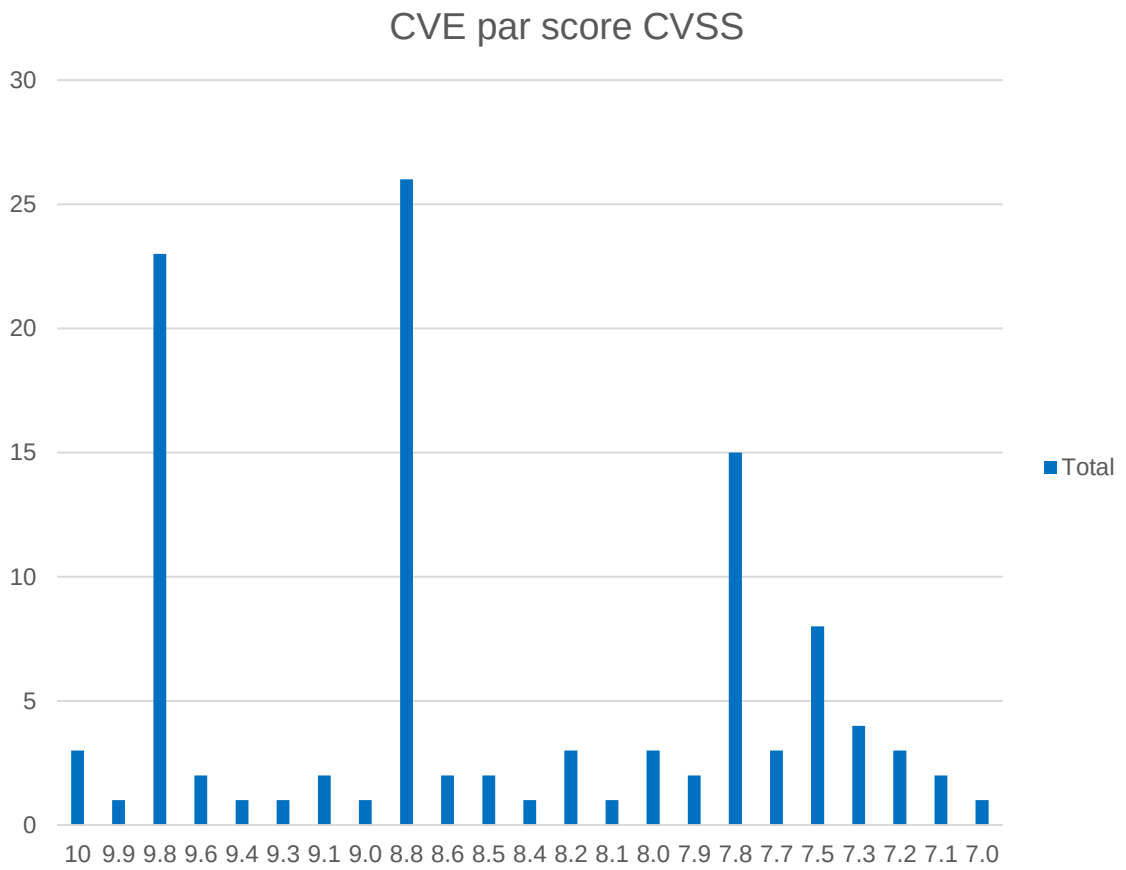
Nombre de CVE par éditeur

110 vulnérabilités ont été analysées et publiées (parmi lesquelles 9 alertes) sur le portail du CERT Santé.



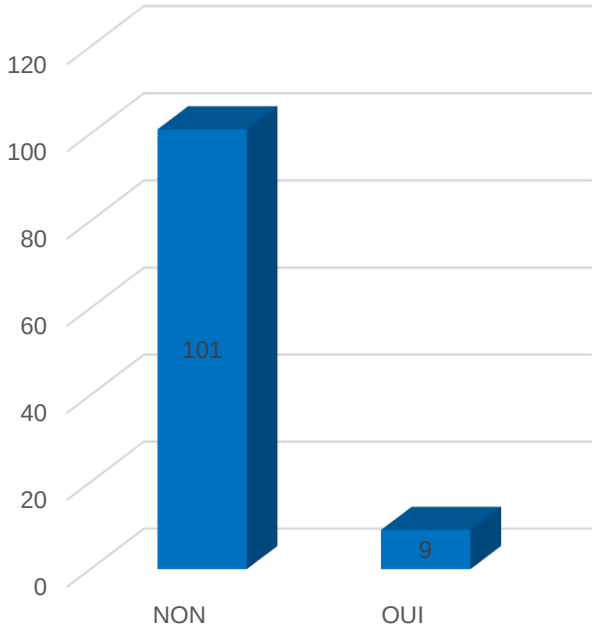
Nombre de CVE par catégorie de produit et score CVSS



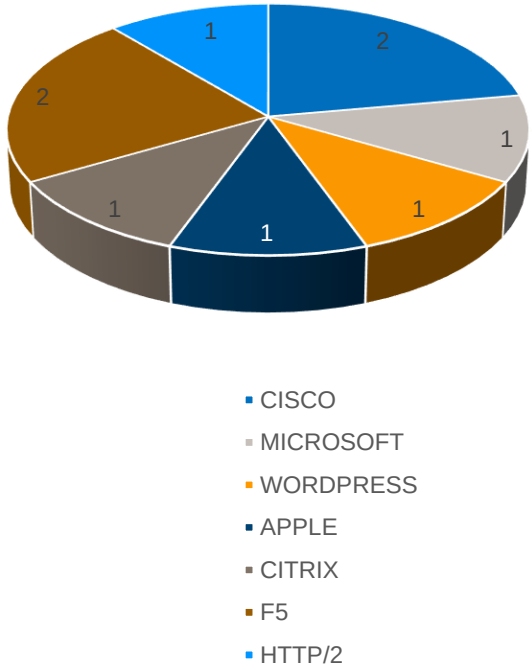


Vulnérabilités exploitées

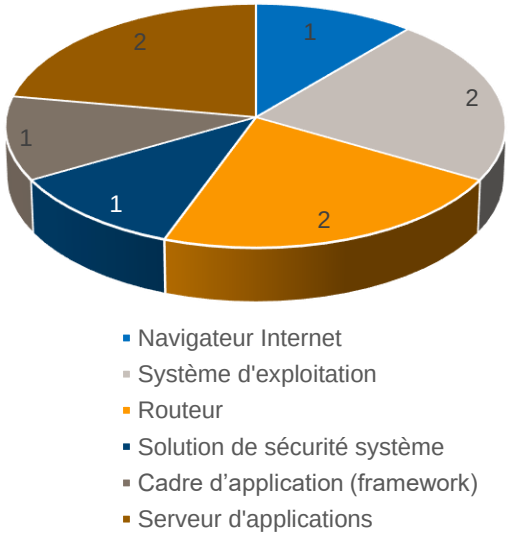
Failles exploitées



Failles exploitées par éditeur



Failles exploitées par type de solution



Les vulnérabilités critiques à surveiller

10

Cisco IOS XE
(CVE-2023-20198)

Contournement de la politique de sécurité

Exploitée

Un attaquant distant et non authentifié peut créer un compte administrateur sur le système.

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

9.4

Citrix Netscaler
(CVE-2023-4966)

Atteinte à la confidentialité

Exploitée

Un attaquant distant et non authentifié peut prendre le contrôle de sessions Netscaler.

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

9.8

VMware vCenter
(CVE-2023-34048)

Exécution de code arbitraire

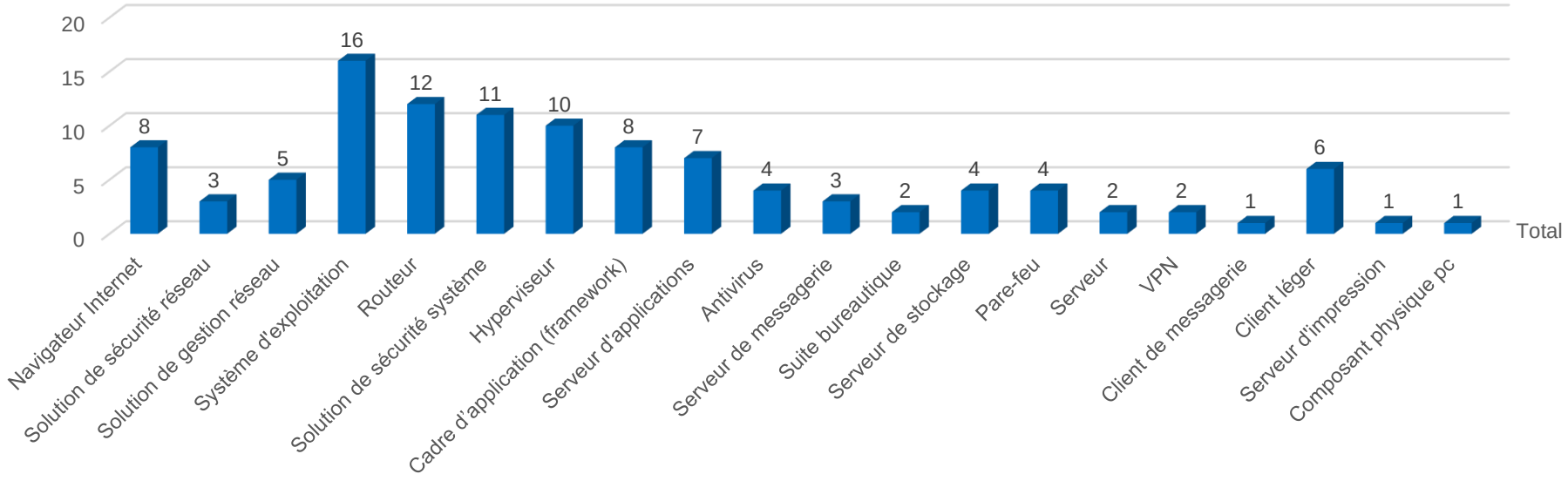
En envoyant des requêtes forgées, un attaquant non authentifié peut exécuter du code sur le vCenter Server.

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

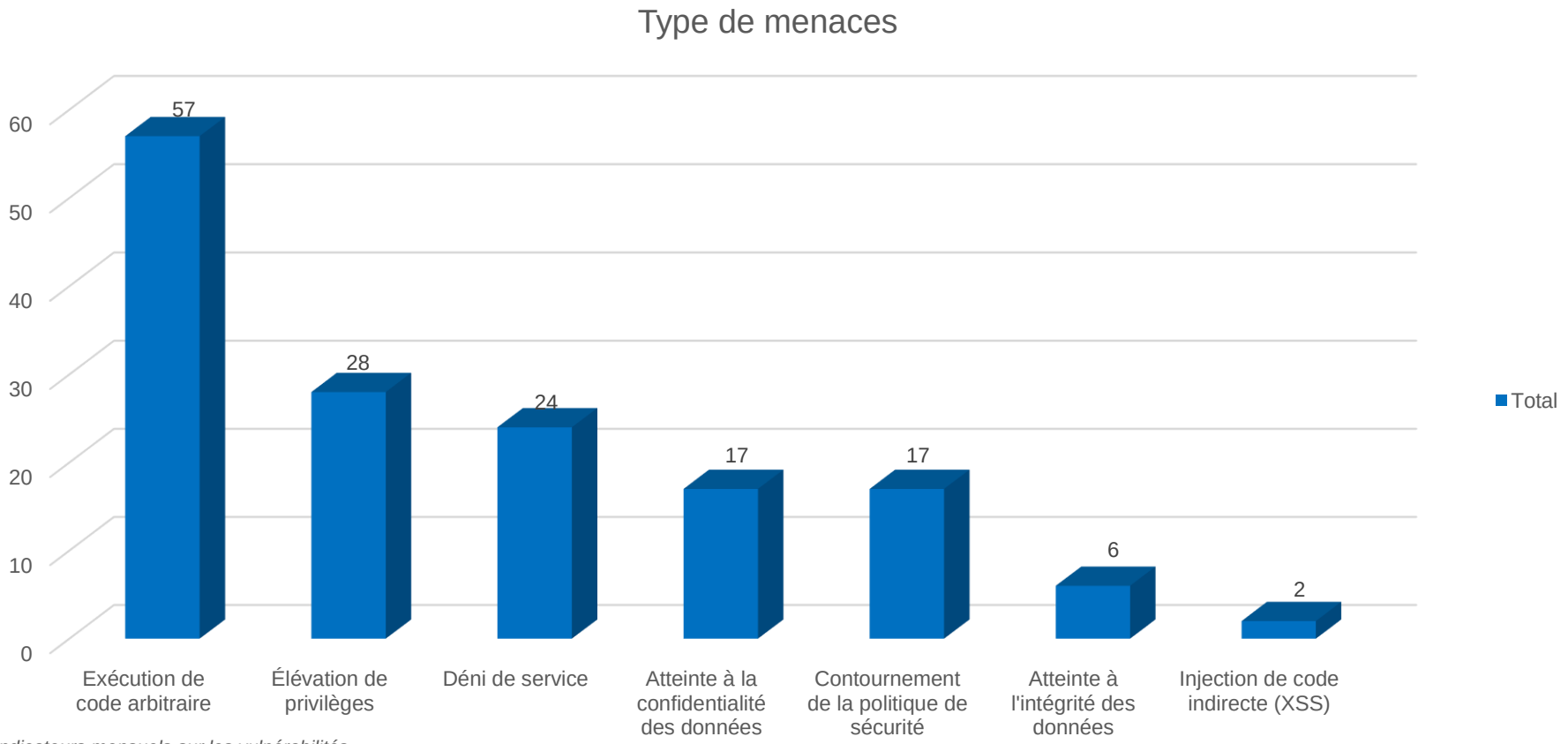
Types de solution vulnérables

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

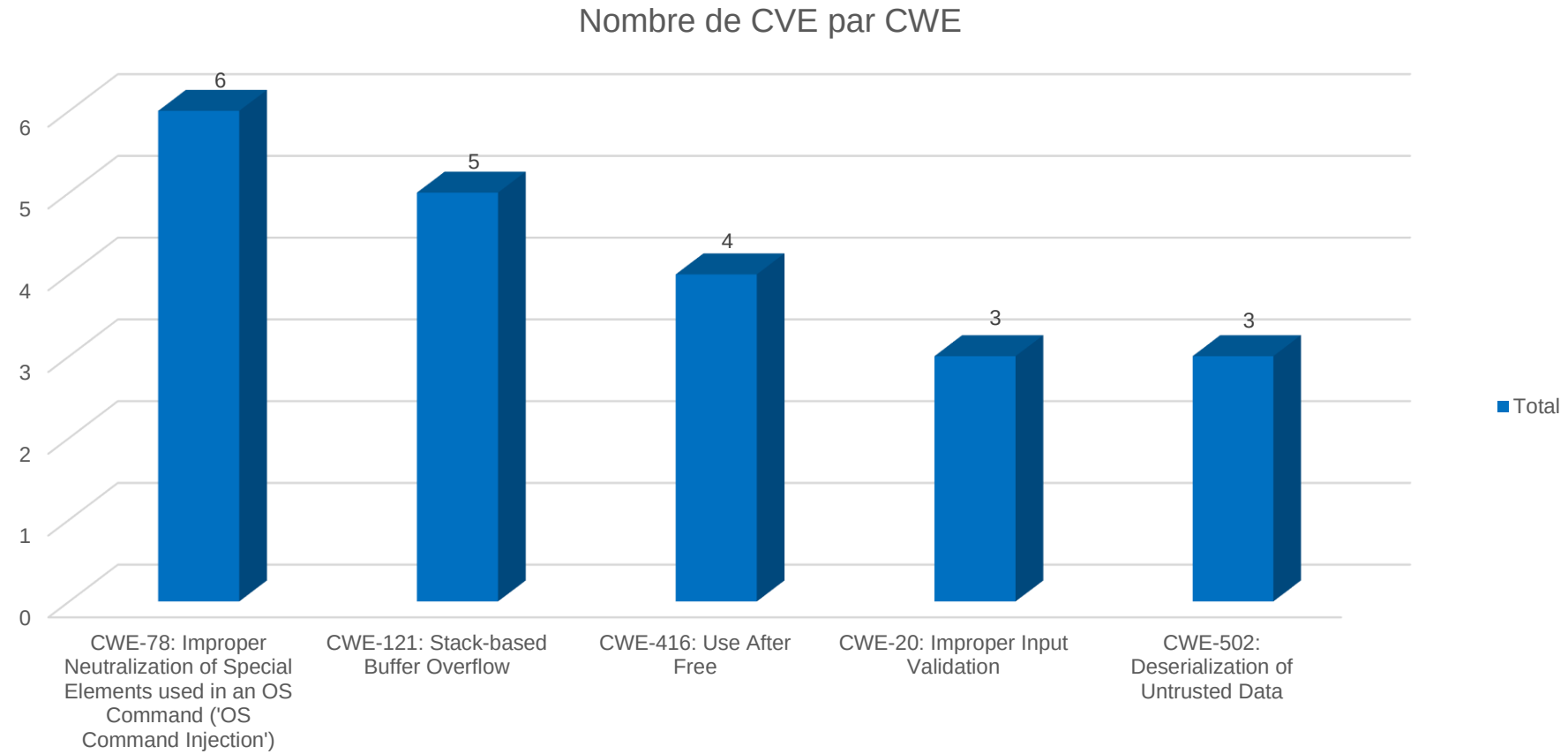
CVE par type de solution



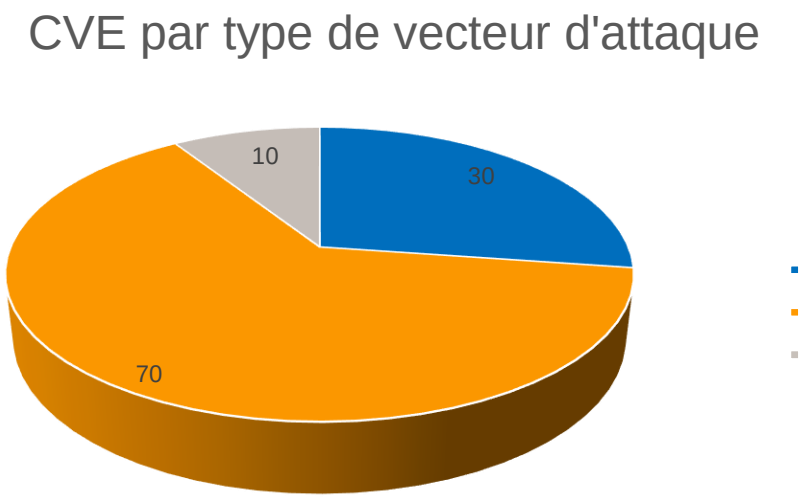
Types de menaces

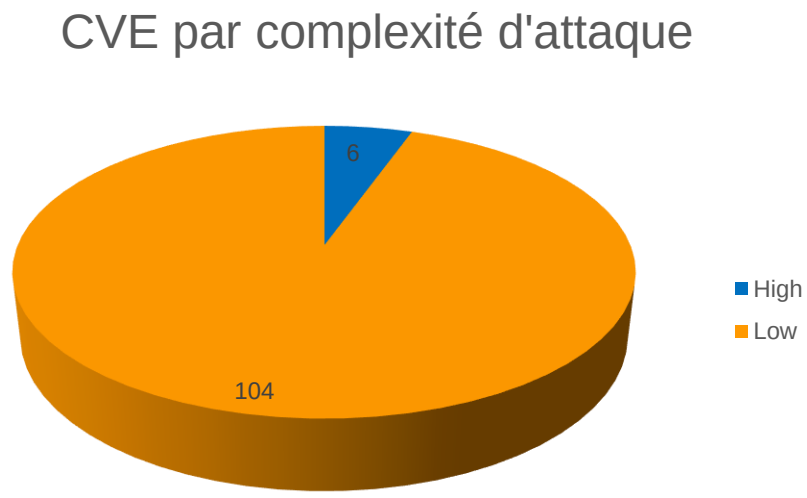


TOP 5 des failles selon le référentiel CWE



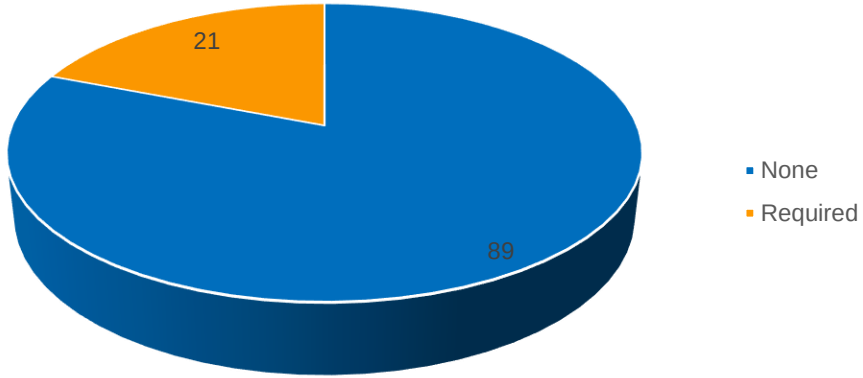
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



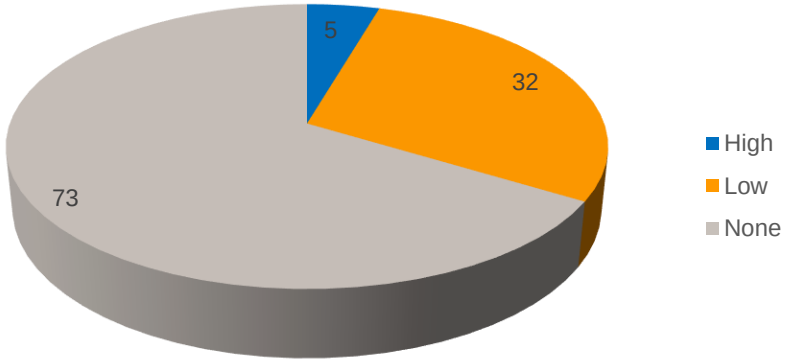


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

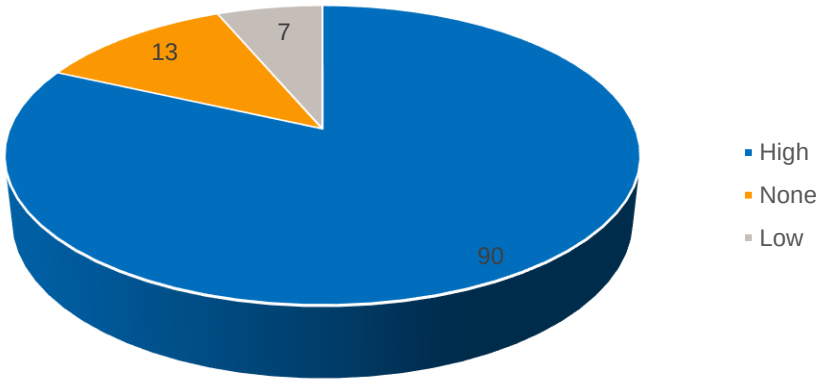


CVE par type de privilège requis

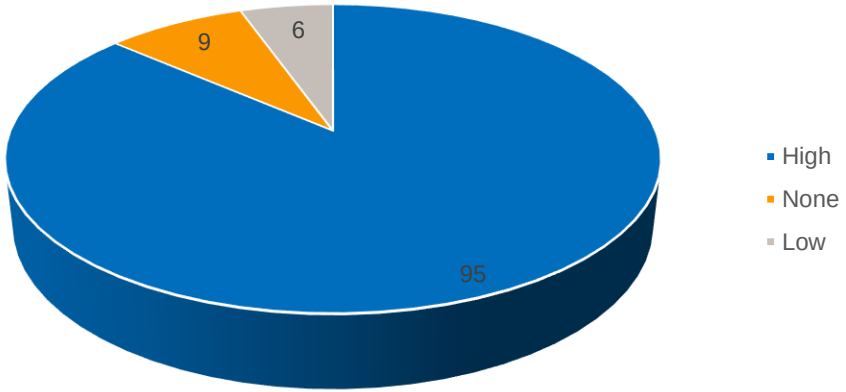


Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données

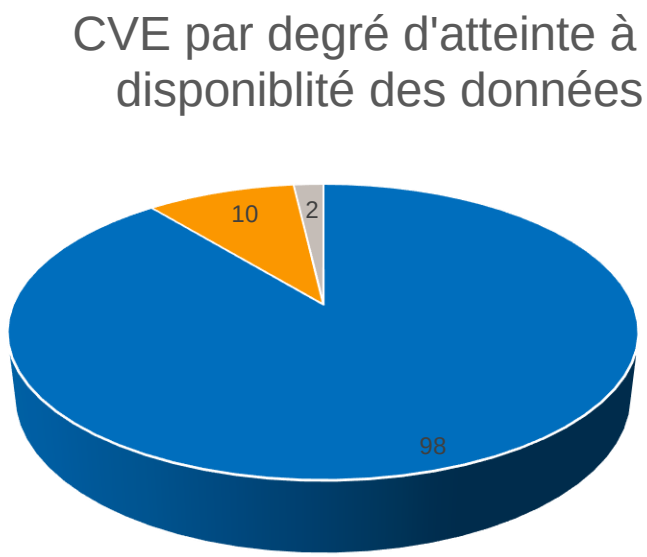
CVE par degré d'atteinte à l'intégrité des données

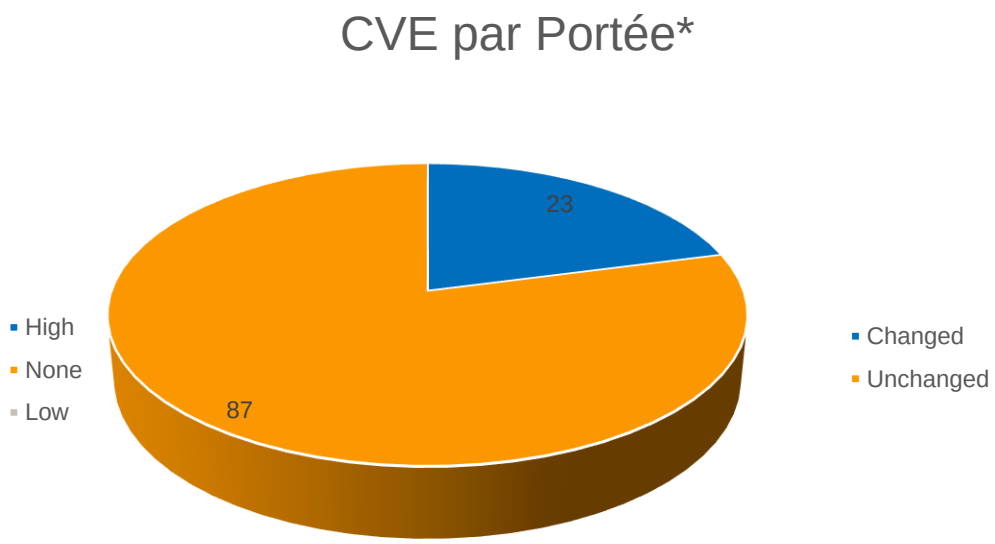


CVE par degré d'atteinte à la confidentialité des données



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.