AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

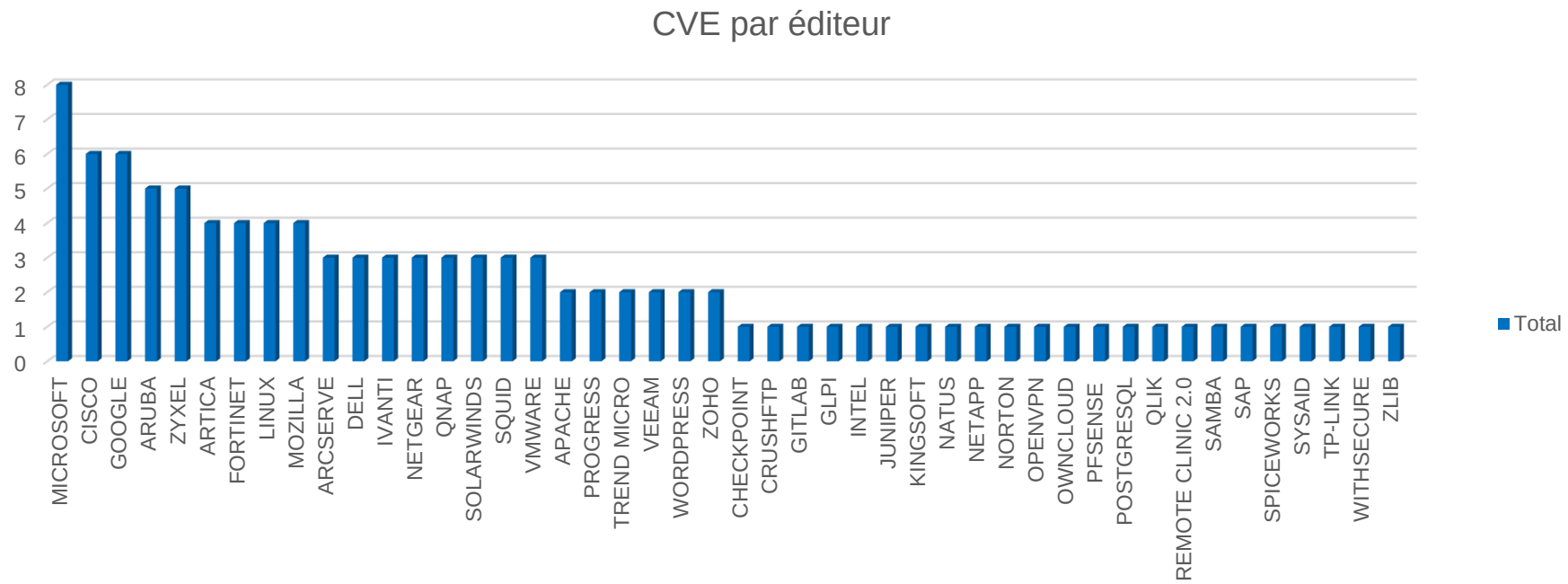
Indicateurs sur la publication des CVE pour le mois de novembre 2023

CERT Santé

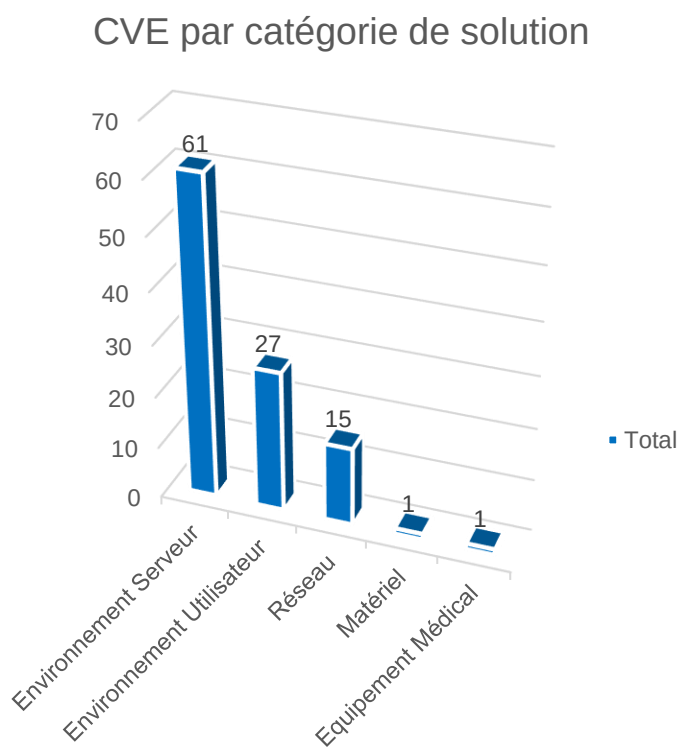
Décembre 2023

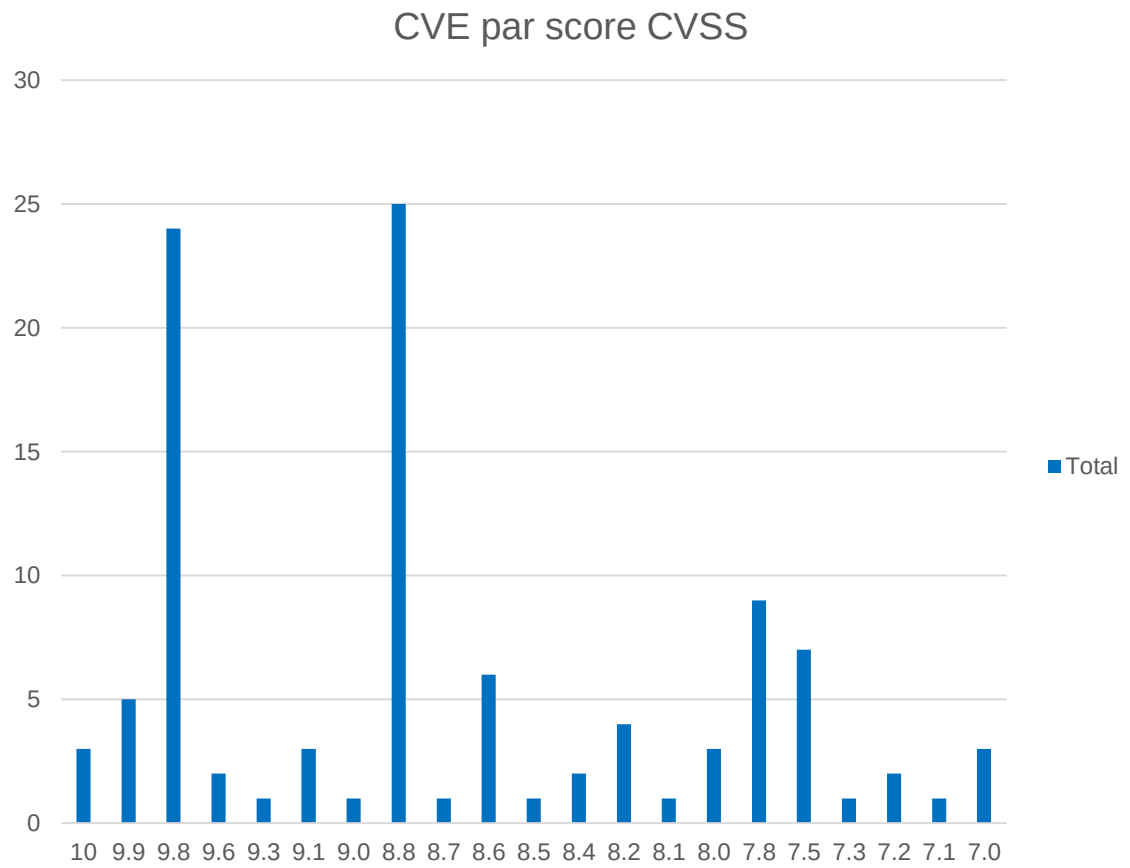
Nombre de CVE par éditeur

105 vulnérabilités ont été analysées et publiées (parmi lesquelles 11 alertes) sur le portail du CERT Santé.



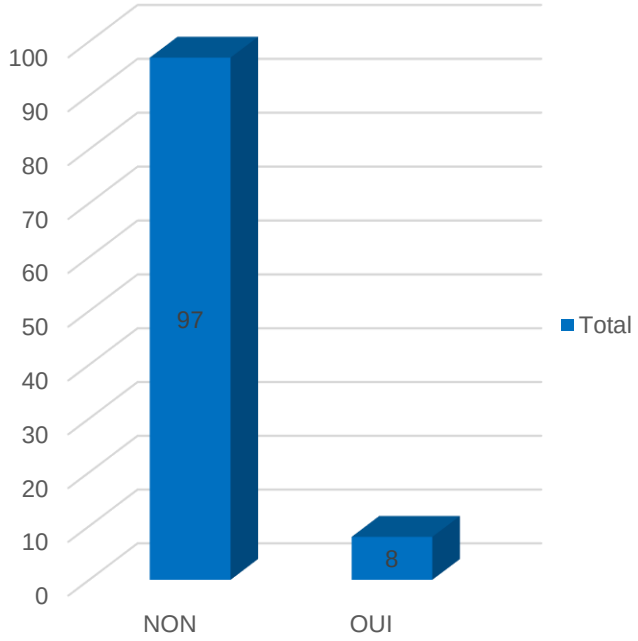
Nombre de CVE par catégorie de produit et score CVSS



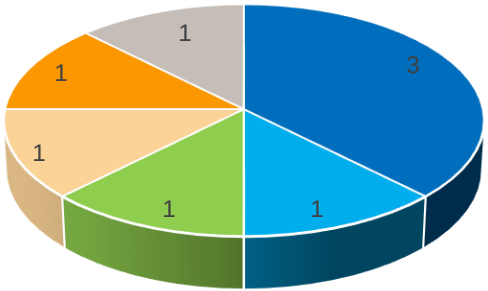


Vulnérabilités exploitées

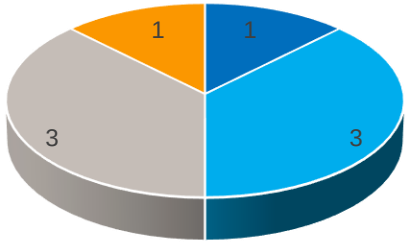
Failles exploitées



Failles exploitées par éditeur



Failles exploitées par type de solution



Les vulnérabilités critiques à surveiller

10

Apache (affectant SolarWinds)
(CVE-2023-46604)

Exécution de code arbitraire

Exploitée

Un attaquant distant et non authentifié peut exécuter du code arbitraire sur le système.

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

10

ownCloud graphapi
(CVE-2023-49103)

Atteinte à la confidentialité

Exploitée

En envoyant des requêtes forgées, un attaquant distant et non authentifié peut voler des données critiques via graphapi.

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

9.6

Qlik Sense Enterprise
(CVE-2023-48365)

Exécution de code arbitraire

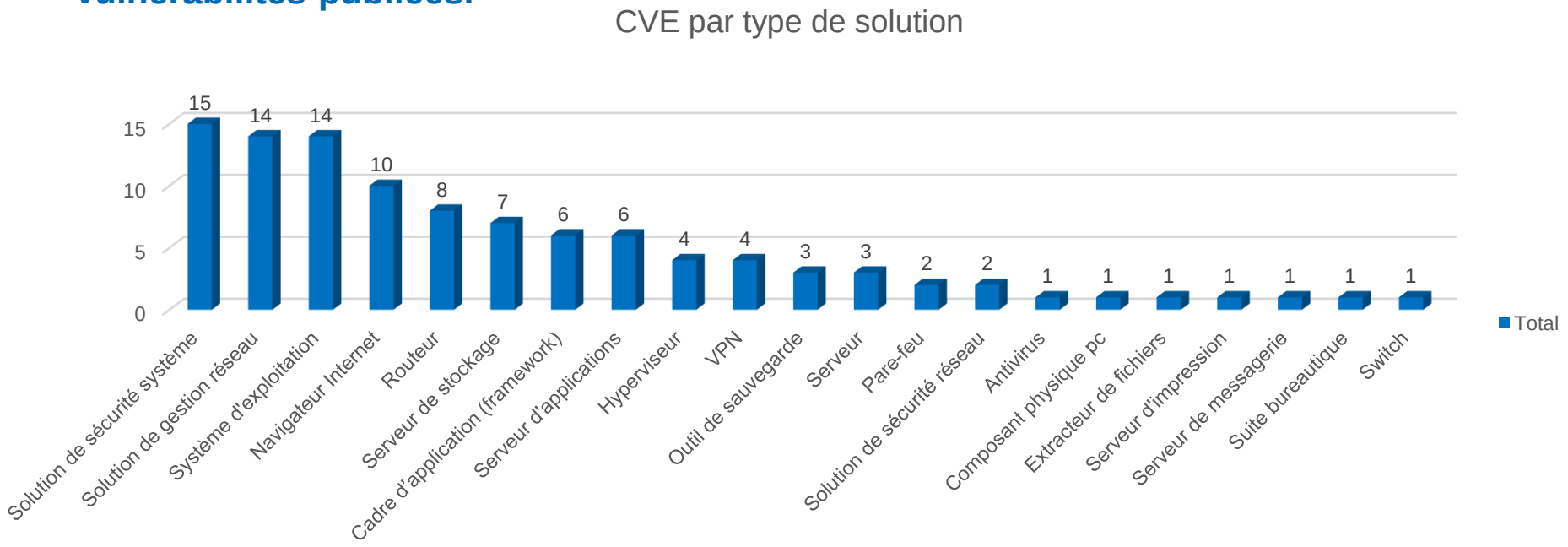
Exploitée

En envoyant des requêtes HTTP forgées, un attaquant distant et non authentifié peut exécuter du code arbitraire.

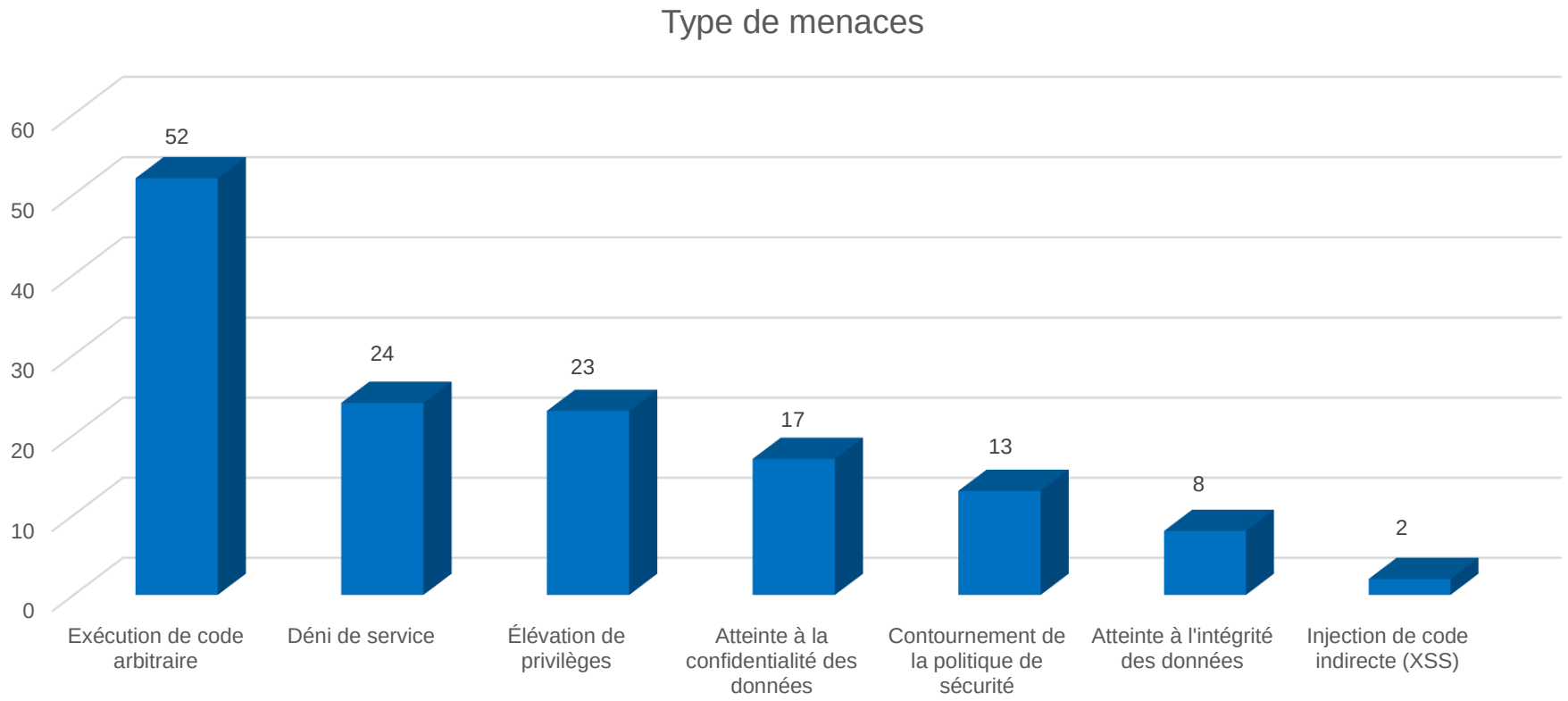
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solution vulnérables

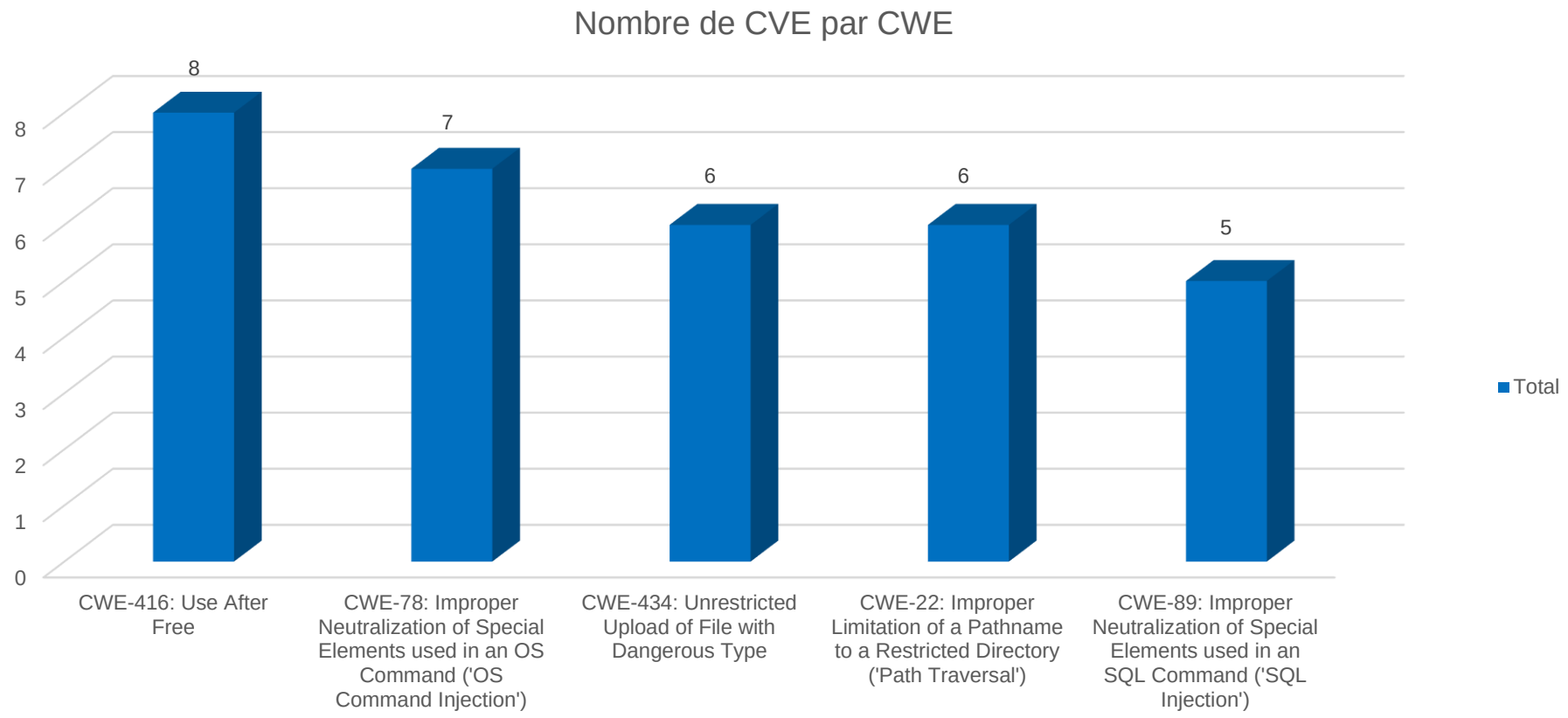
Les solutions de sécurité système, les solutions de gestion réseau et les systèmes d'exploitation sont les principaux types d'équipements affectés par les vulnérabilités publiées.



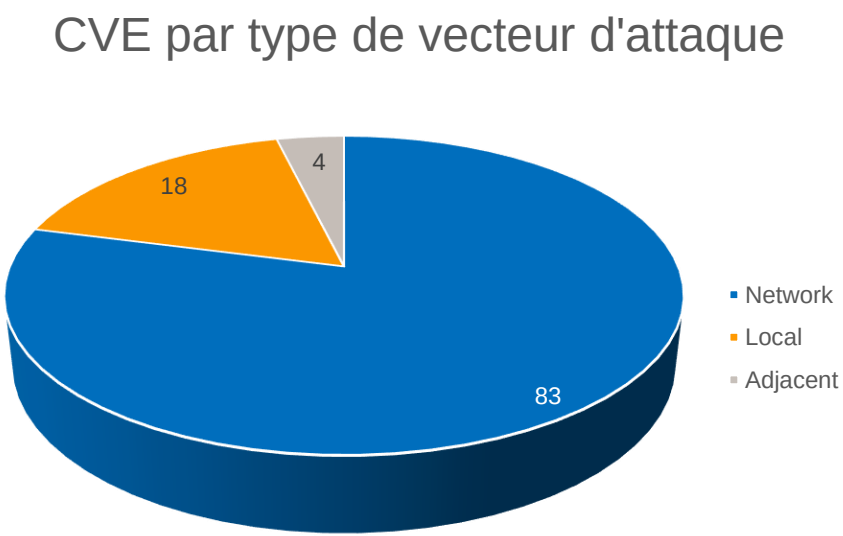
Types de menaces

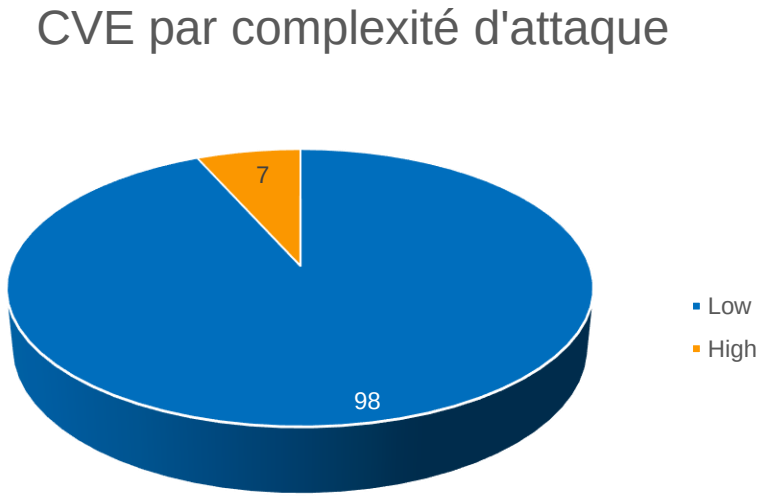


TOP 5 des failles selon le référentiel CWE



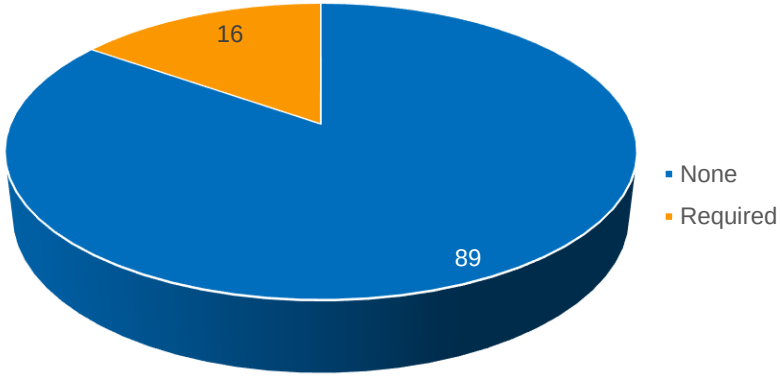
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



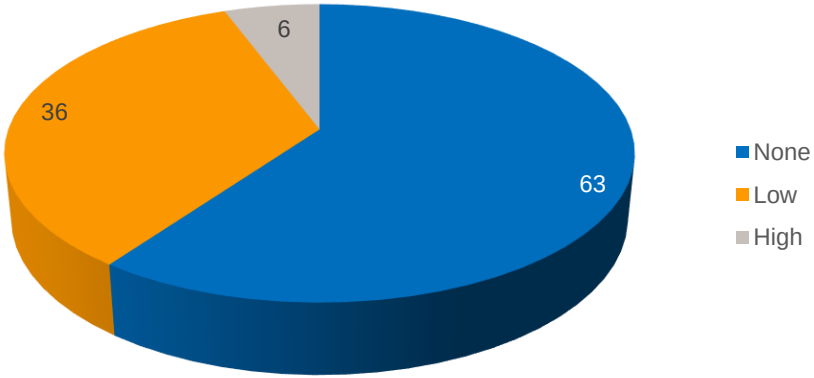


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

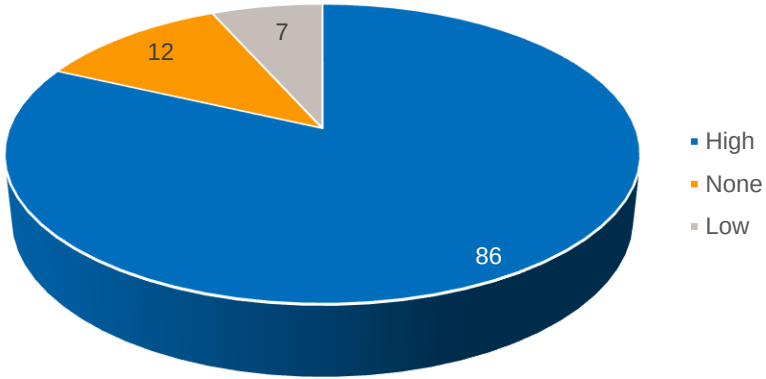


CVE par type de privilège requis

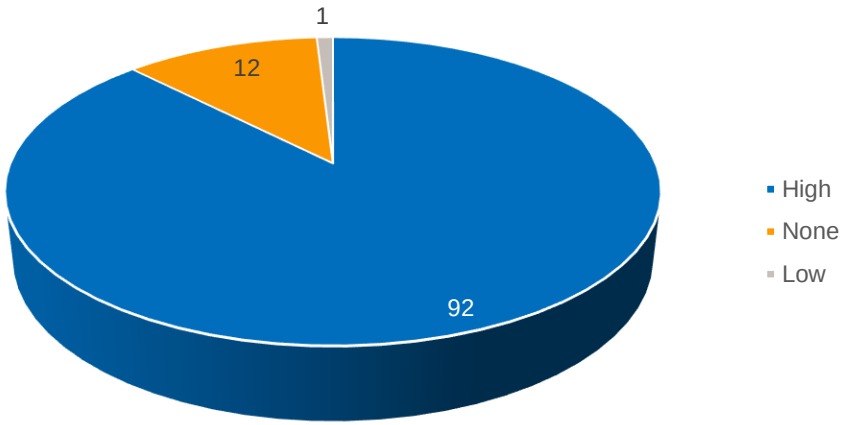


Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données

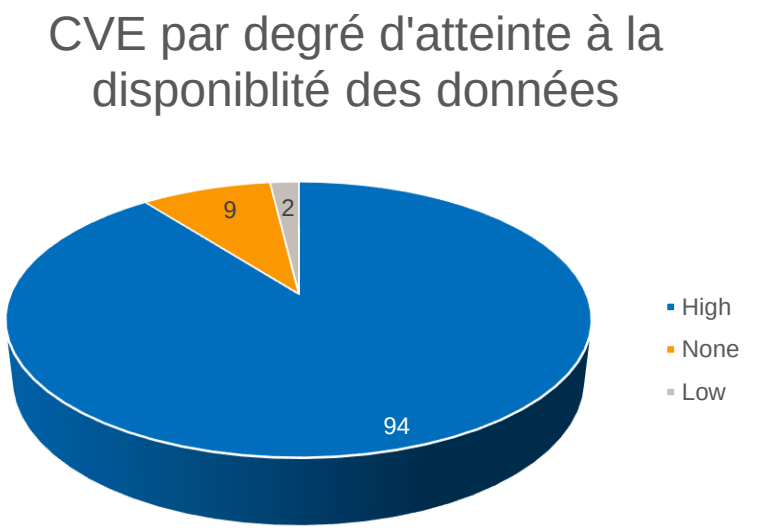
CVE par degré d'atteinte à l'intégrité des données

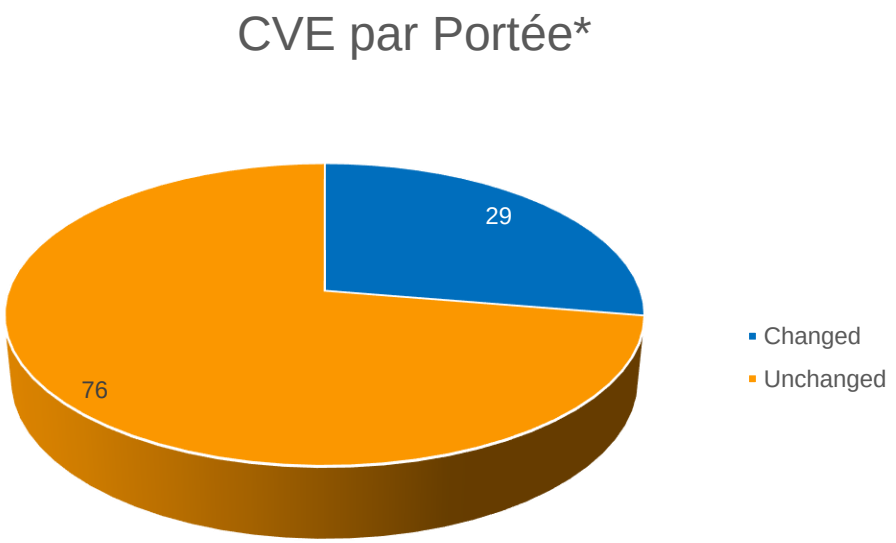


CVE par degré d'atteinte à la confidentialité des données



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.