AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

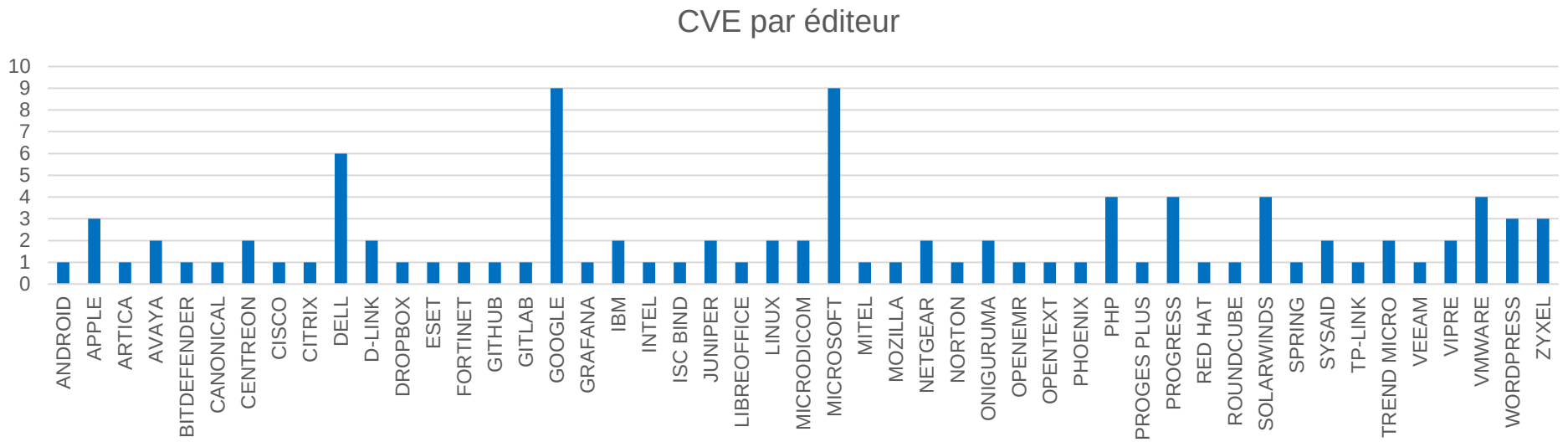
Indicateurs sur la publication des CVE pour le mois de juin 2024

CERT Santé

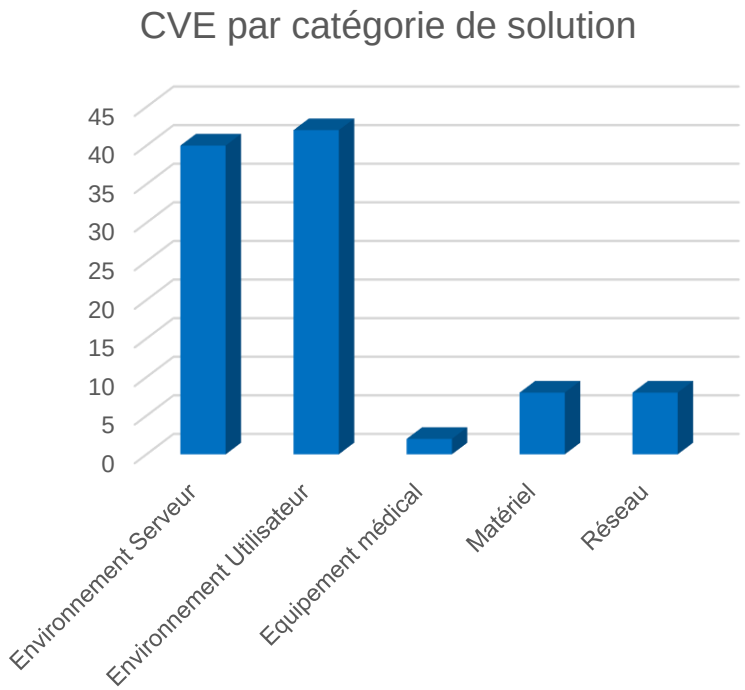
Juillet 2024

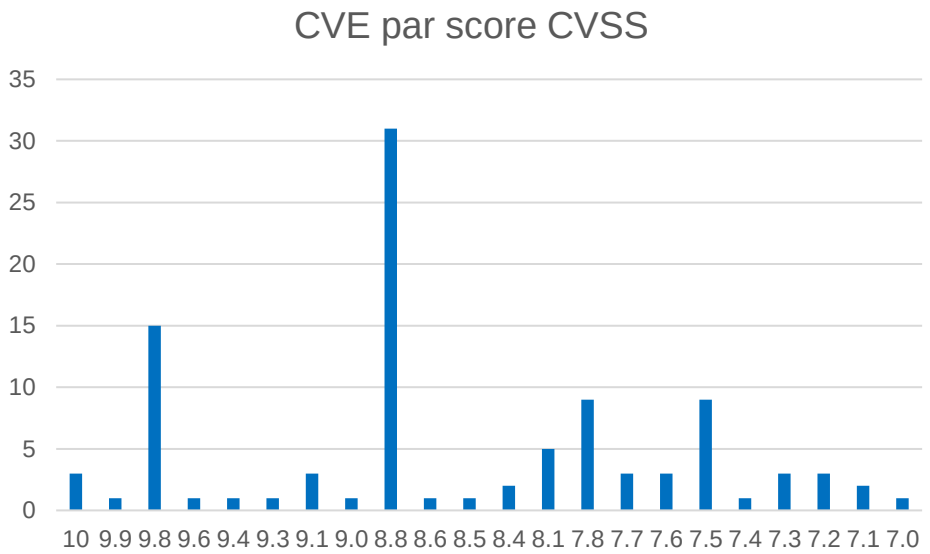
Nombre de CVE par éditeur

100 vulnérabilités ont été analysées et publiées (parmi lesquelles 5 alertes) sur le portail du CERT Santé.

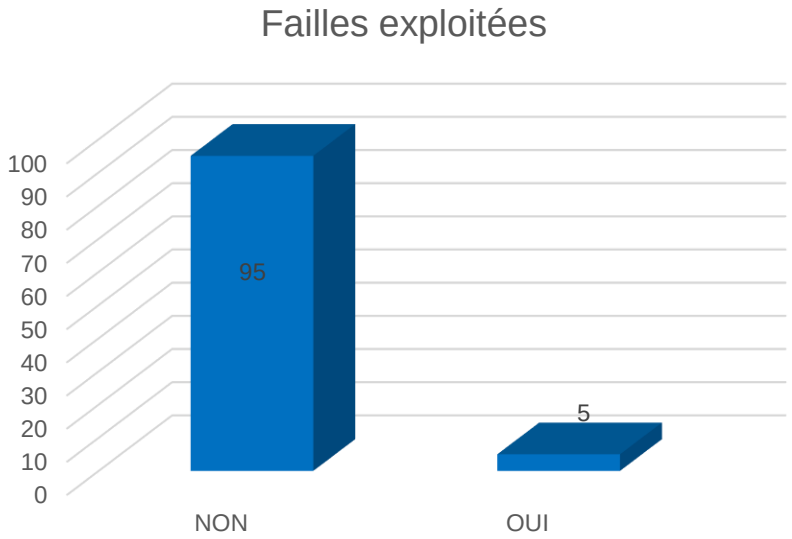


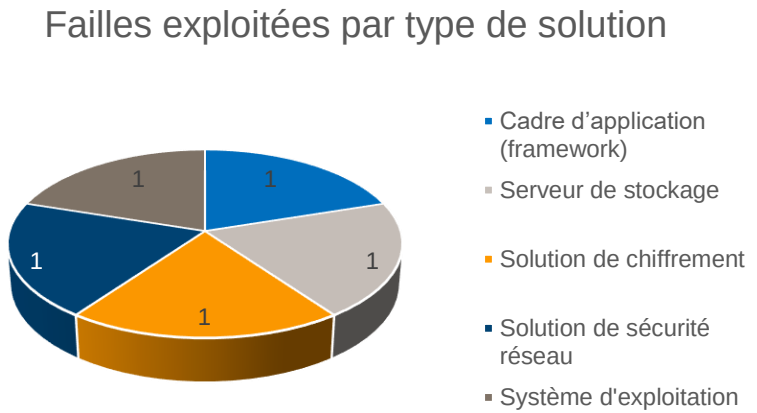
Nombre de CVE par catégorie de produit et score CVSS

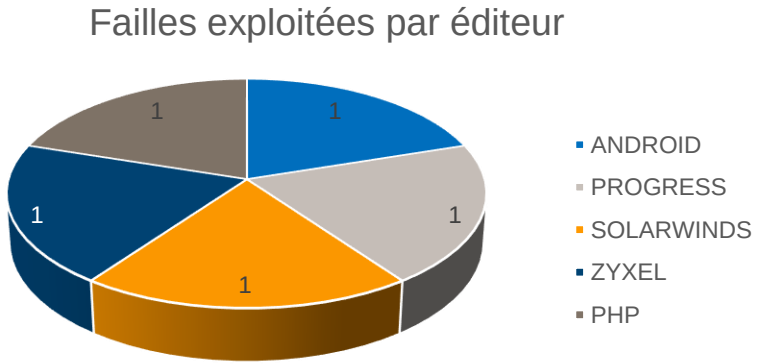




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

9.8

Zyxel

Exécution de code arbitraire

Exploitée

(CVE-2024-29973)

Un défaut dans le paramètre « setCookie » de Zyxel NAS326 and NAS542 permet à un attaquant non authentifié, en envoyant des requêtes HTTP POST spécifiquement forgées, d'exécuter du code arbitraire.

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

9.1

Progress

Contournement de la politique de sécurité

Exploitée

(CVE-2024-5806)

Un défaut de contrôle de l'authentification dans Progress MOVEit Transfer permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'usurper le compte d'un utilisateur.

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

9.8

PHP

Exécution de code arbitraire

Exploitée

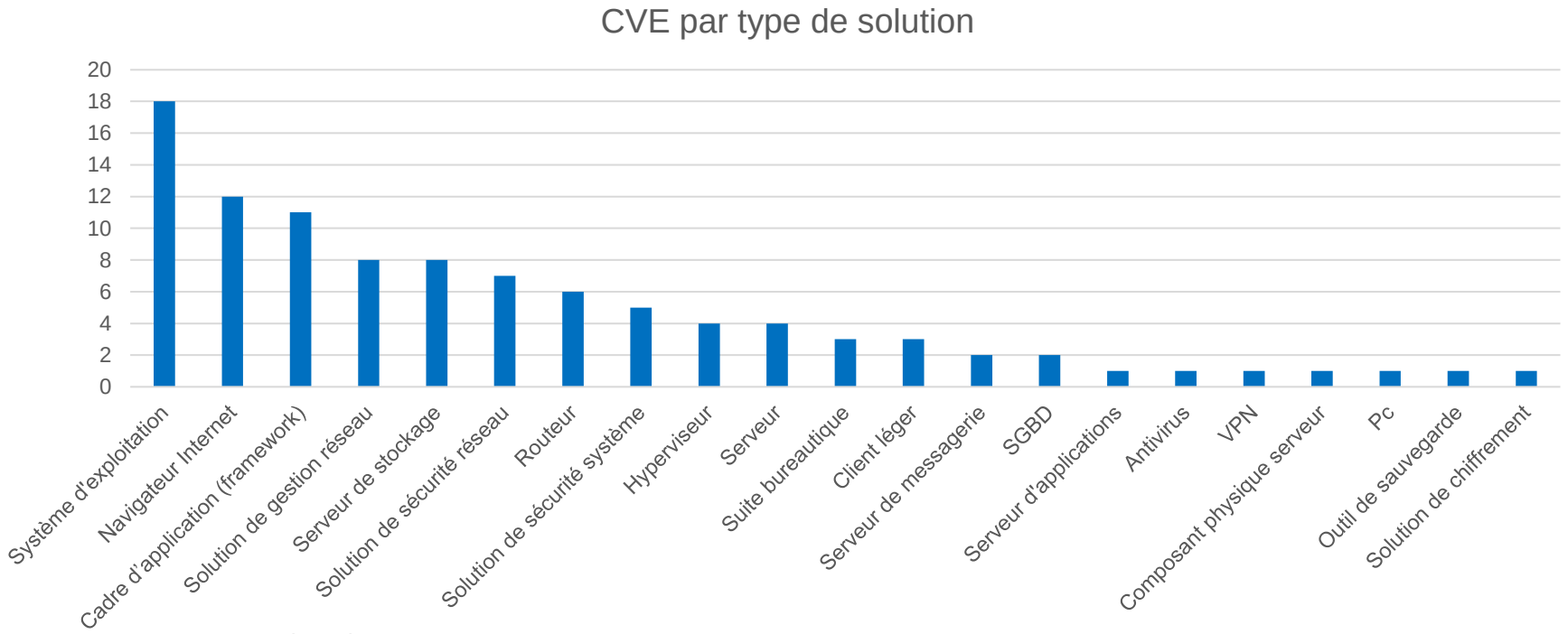
(CVE-2024-4577)

Un défaut de gestion des caractères dans la fonction Best-Fit de Windows utilisant le module PHP CGI permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire sur le système.

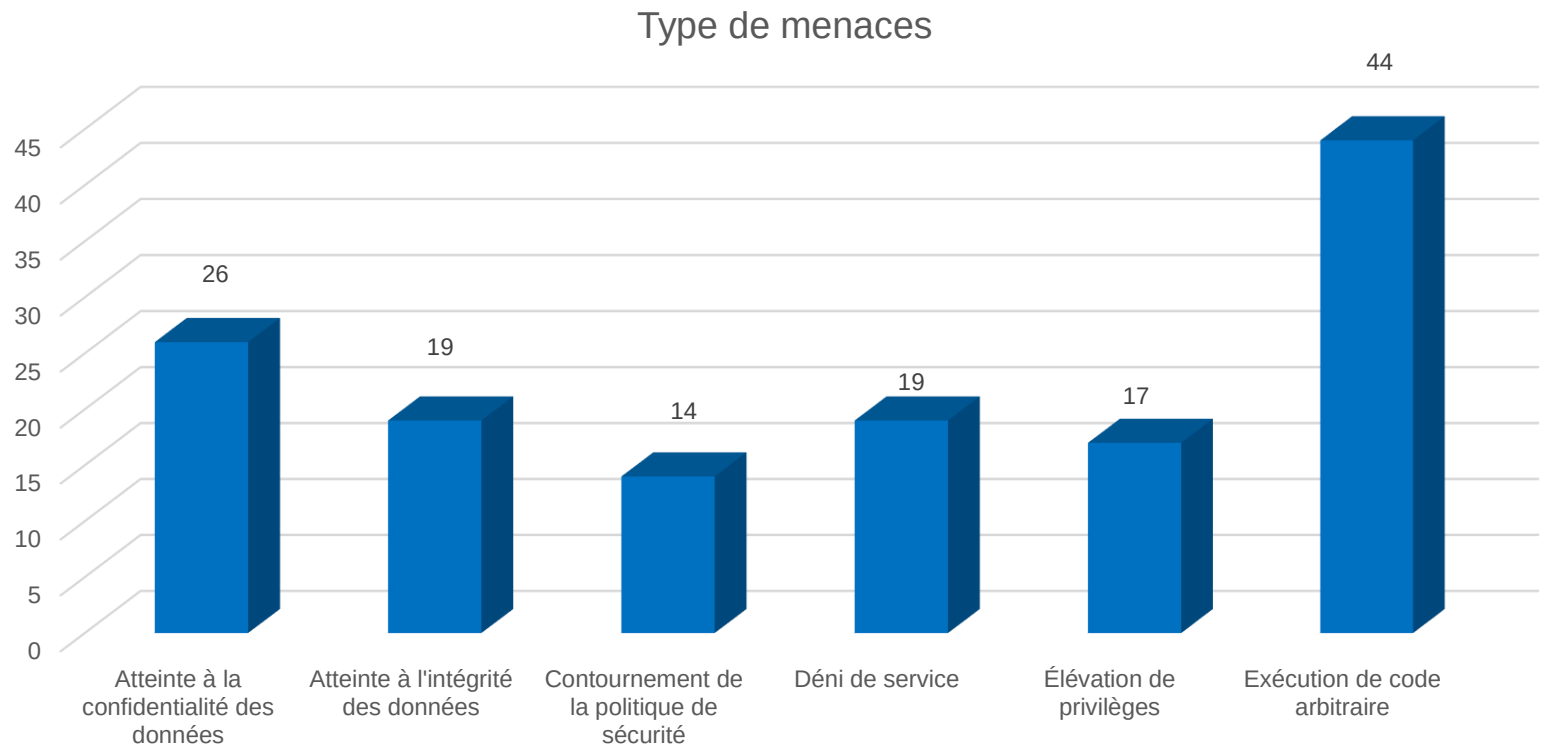
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

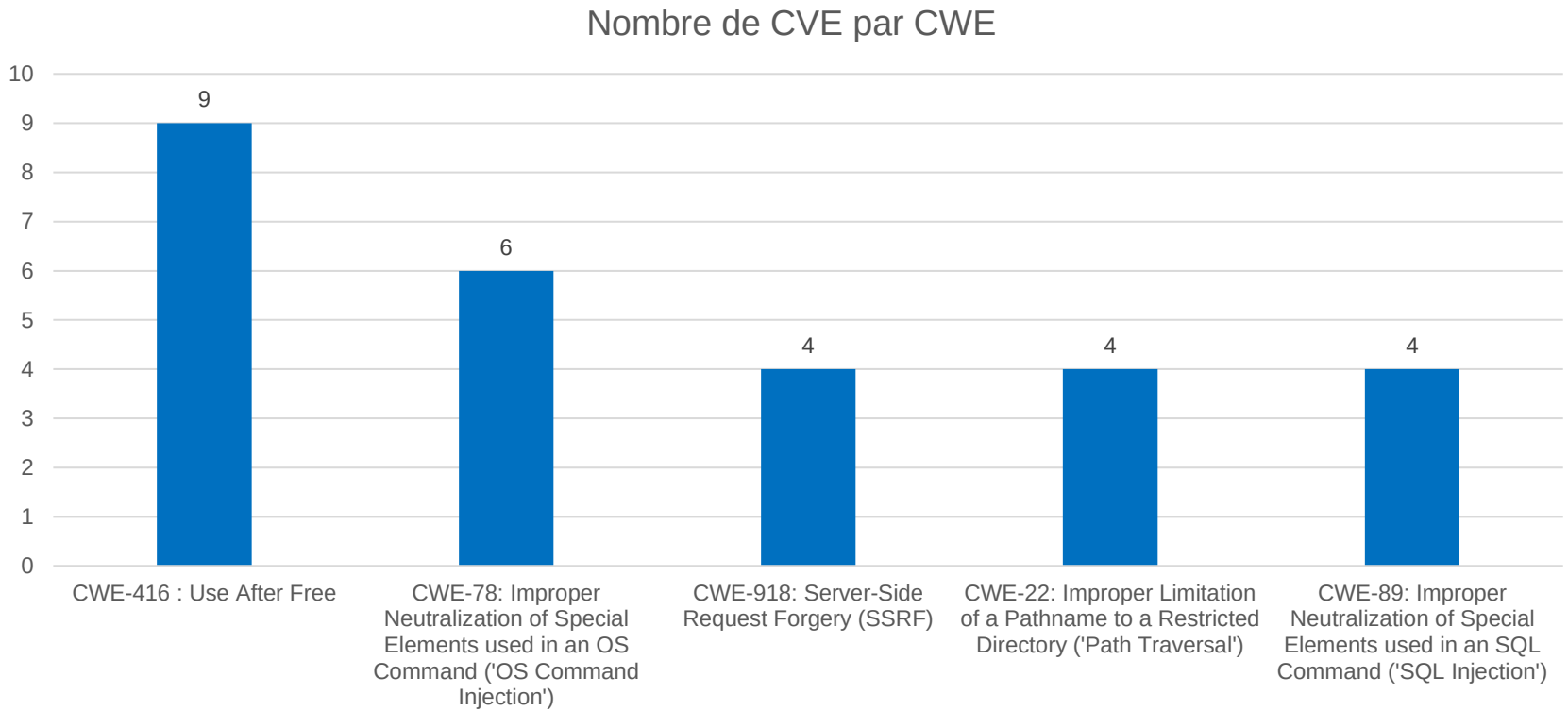
Les systèmes d'exploitation, les navigateurs internet et les cadres d'application (framework) sont les principaux types d'équipements affectés par les vulnérabilités publiées.



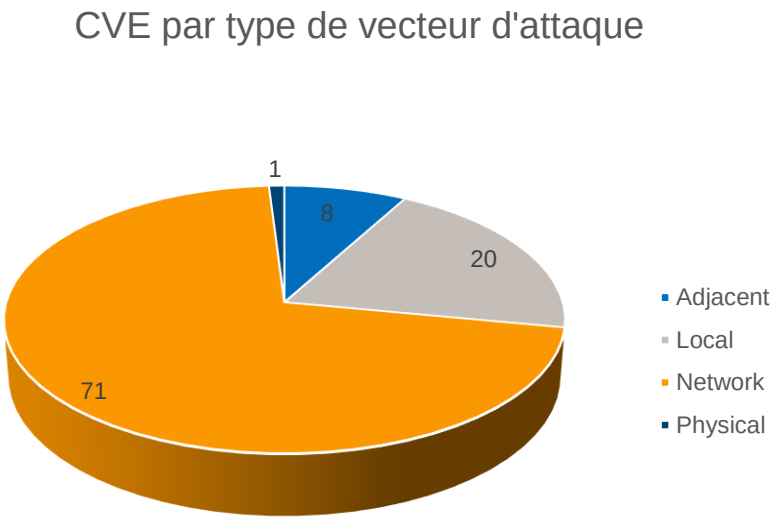
Types de menaces

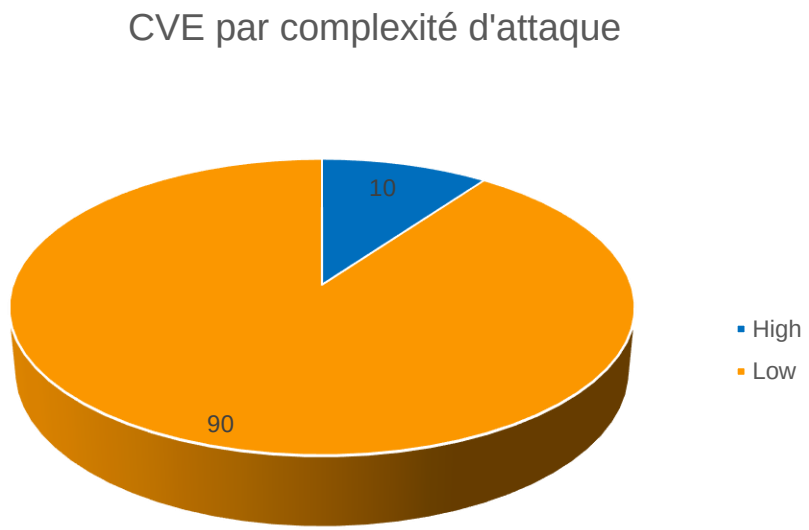


TOP 5 des failles selon le référentiel CWE



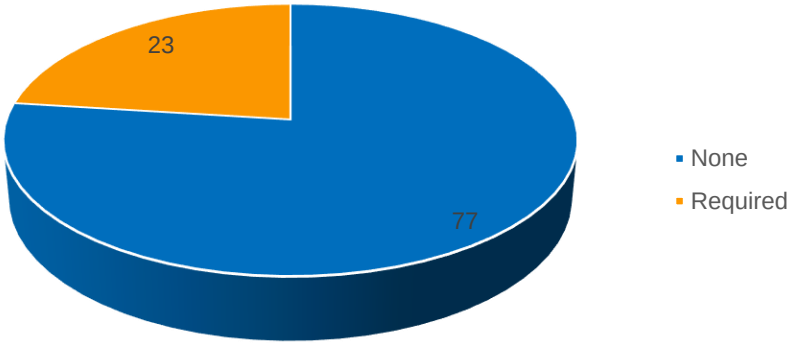
Nombre de CVE selon le vecteur d’attaque et la complexité de l’attaque



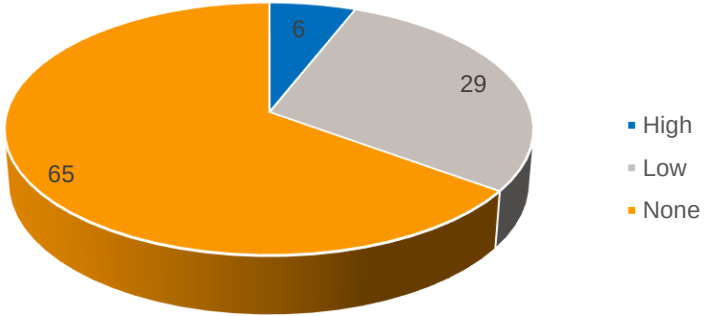


Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

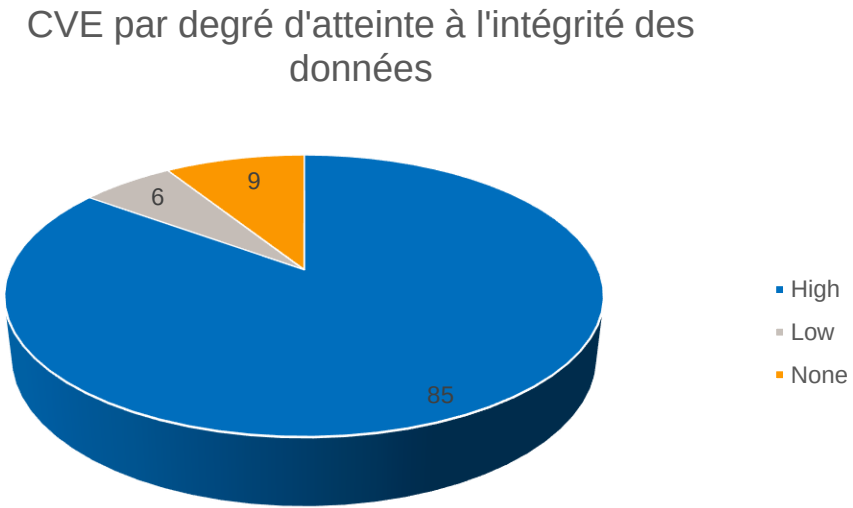
CVE par interaction utilisateur

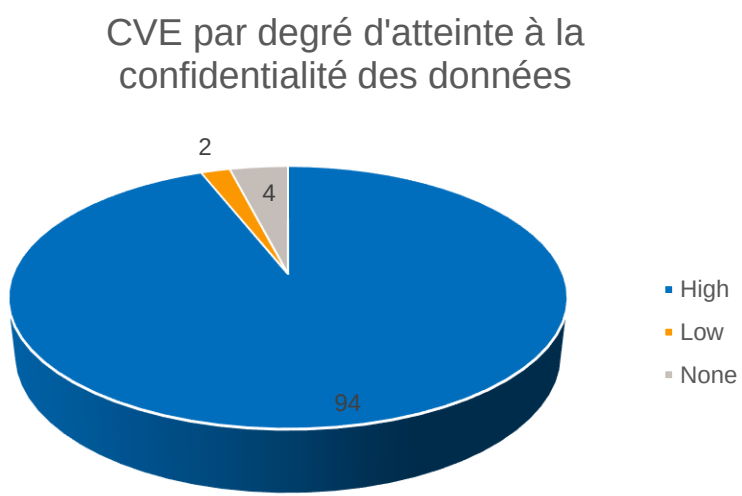


CVE par type de privilèges requis

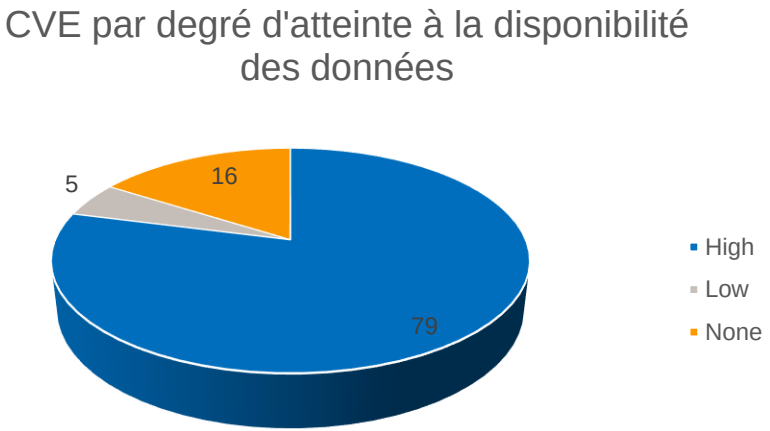


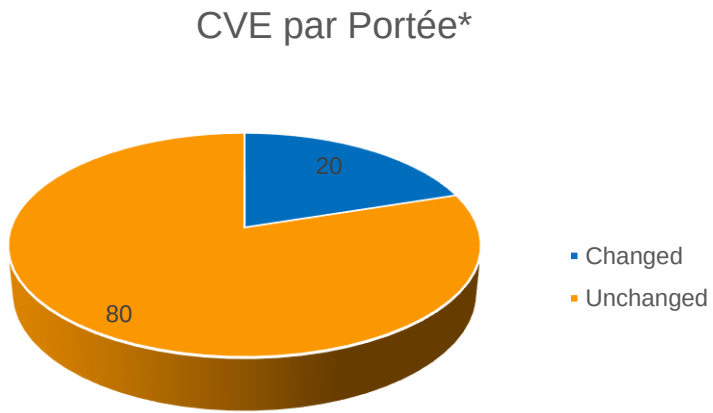
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données





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.