AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

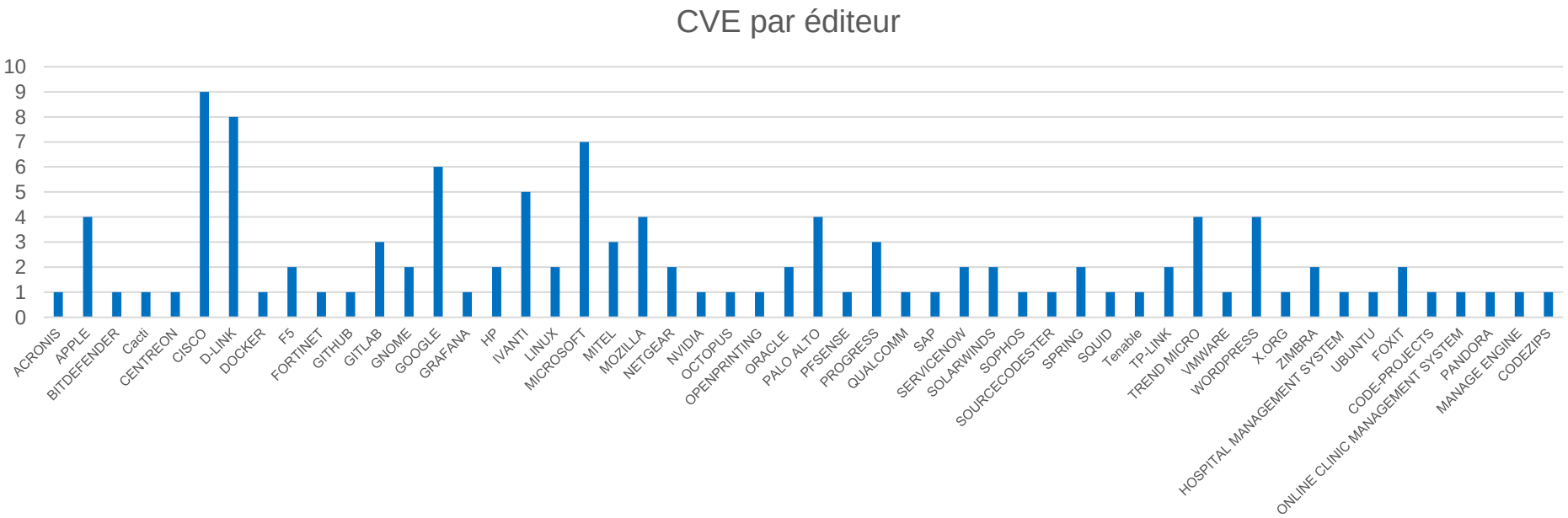
Indicateurs sur la publication des CVE pour le mois d'octobre 2024

CERT Santé

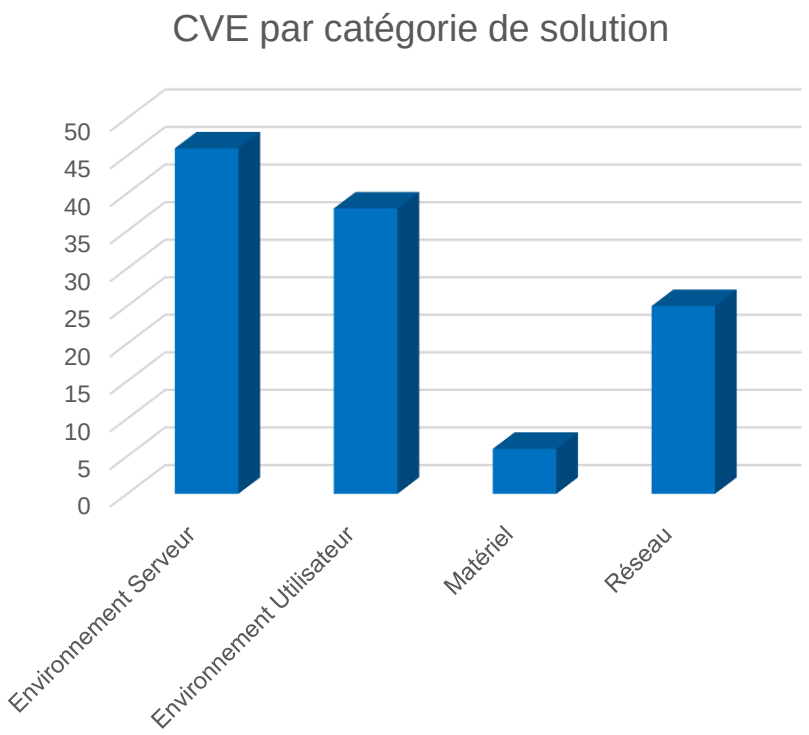
Novembre 2024

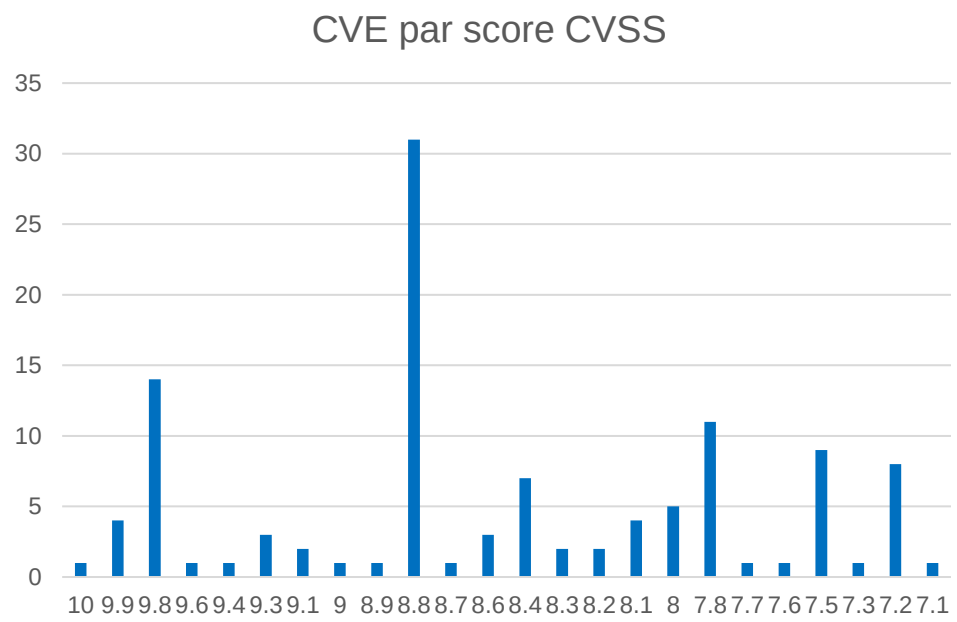
Nombre de CVE par éditeur

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

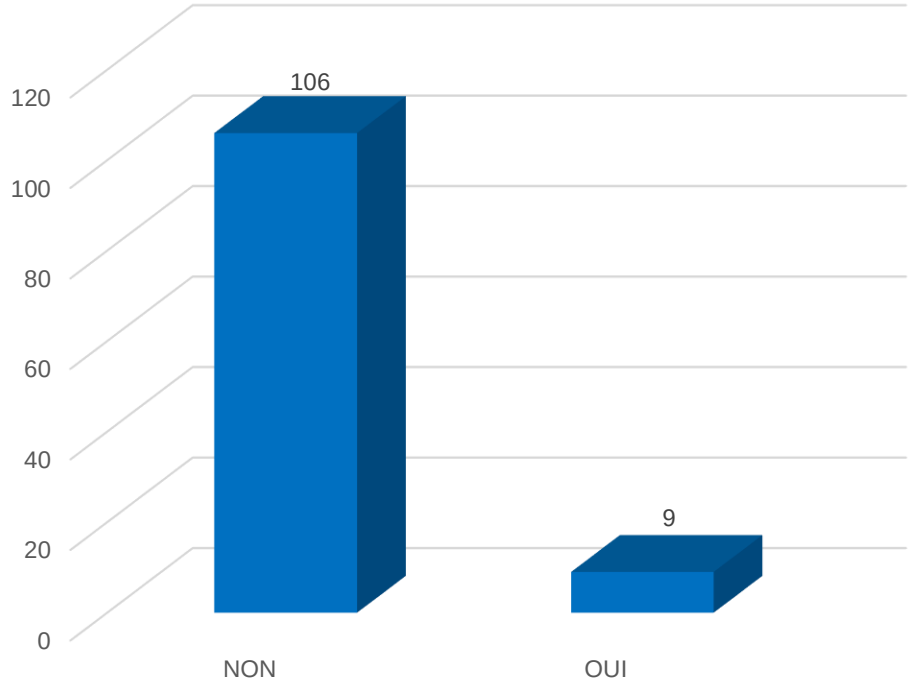


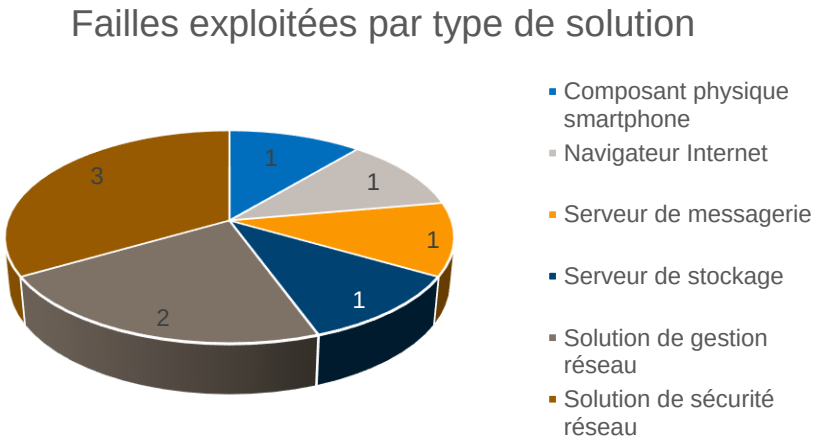
Nombre de CVE par catégorie de produit et score CVSS

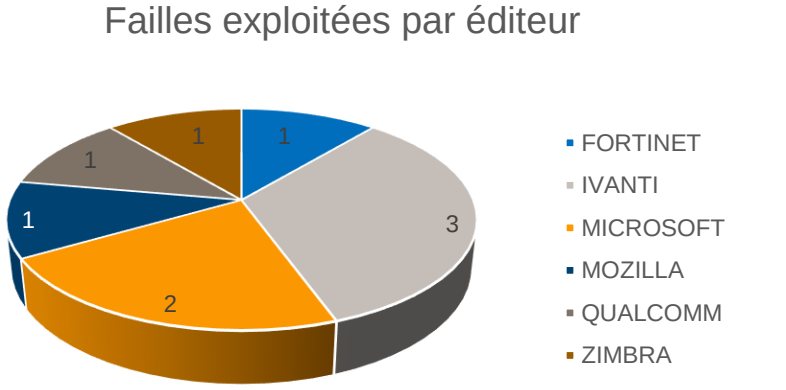




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

10

Zimbra

(CVE-2024-45519)

Exécution de code arbitraire | Exploitée | PoC

L'exploitation d'une vulnérabilité dans le service postjournal de Zimbra Collaboration permet à un attaquant non authentifié d'exécuter des commandes arbitraires.

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

9.8

Fortinet

(CVE-2024-47575)

Exécution de code arbitraire | Exploitée | PoC

Une absence d'authentification dans la fonction critique fgfmd daemon de FortiManager 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.

8.8

Mozilla

(CVE-2024-9680)

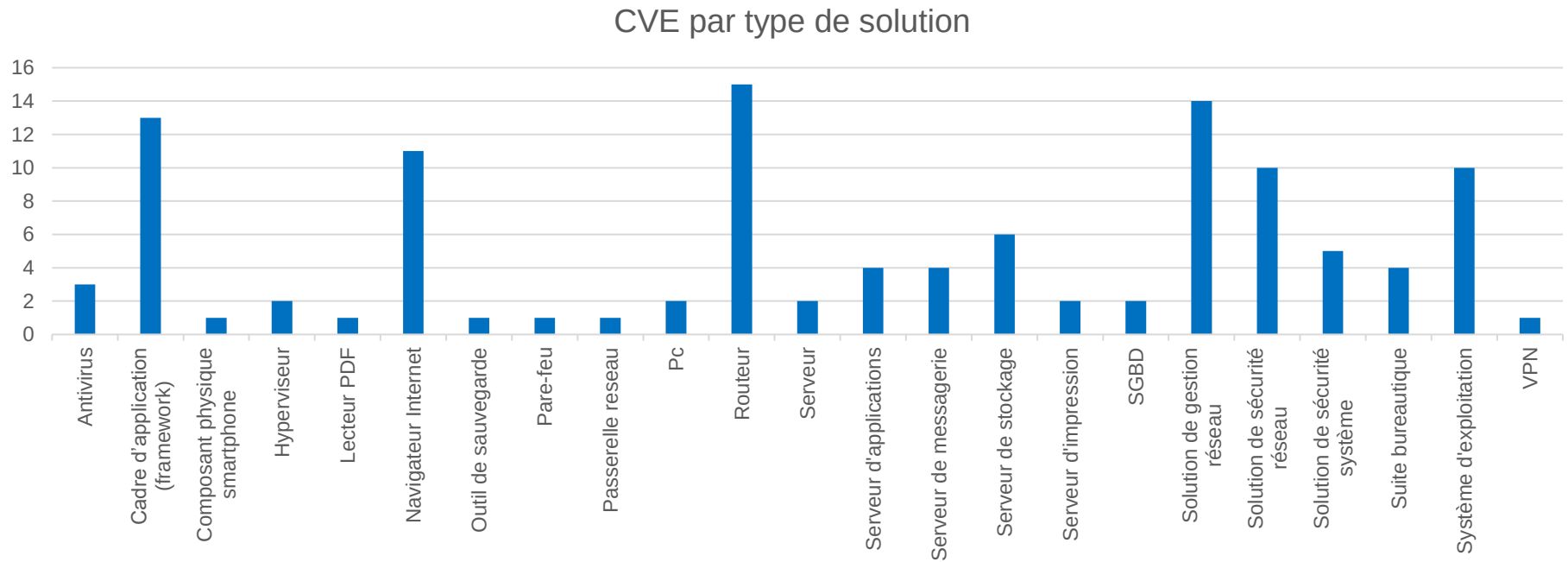
Exécution de code arbitraire | Exploitée

Un défaut de libération de la mémoire dans le composant Animation timelines de Mozilla Firefox permet à un attaquant non authentifié, en persuadant une victime de consulter un site web spécifiquement forgé, d'exécuter du code arbitraire.

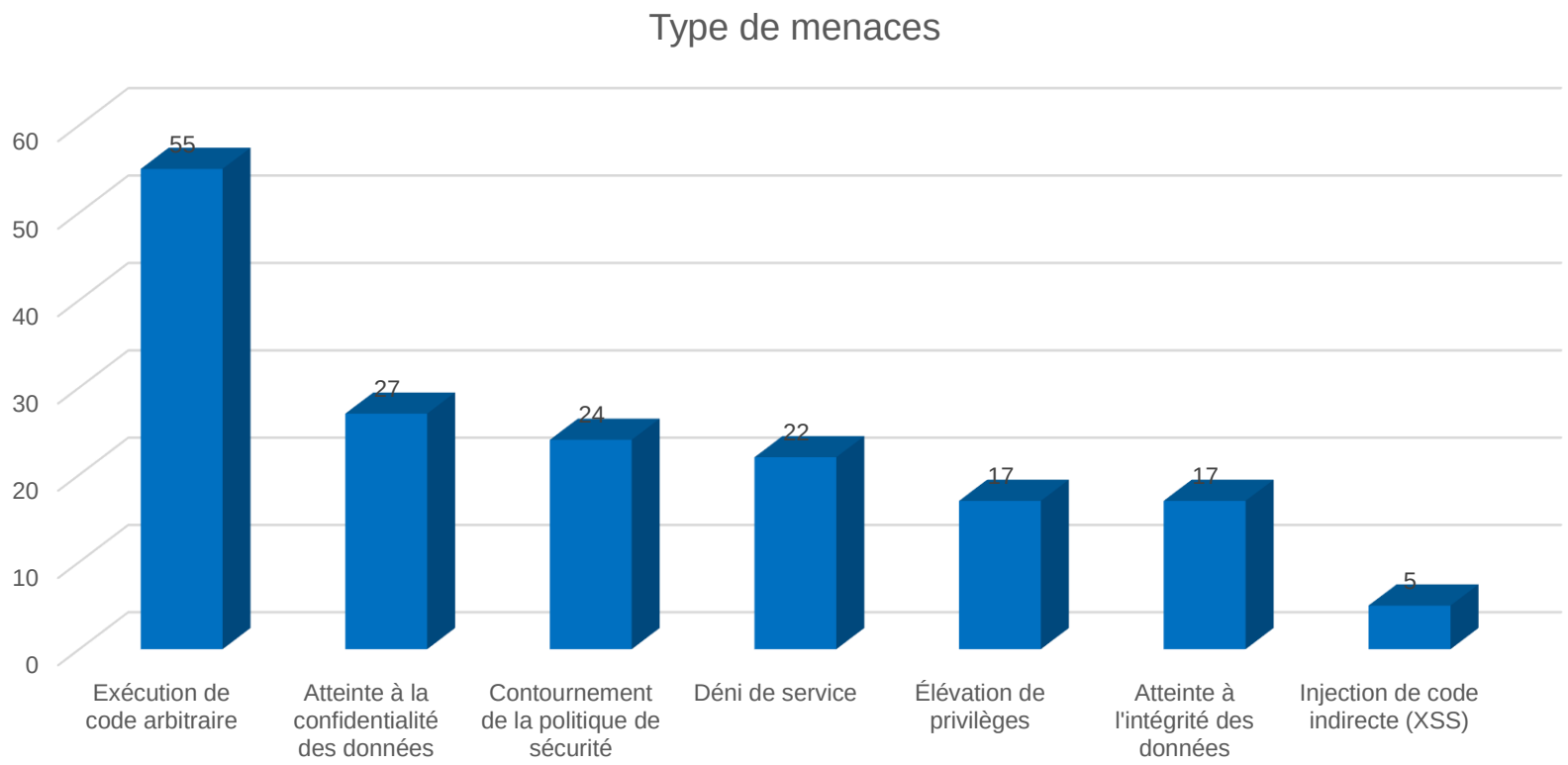
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

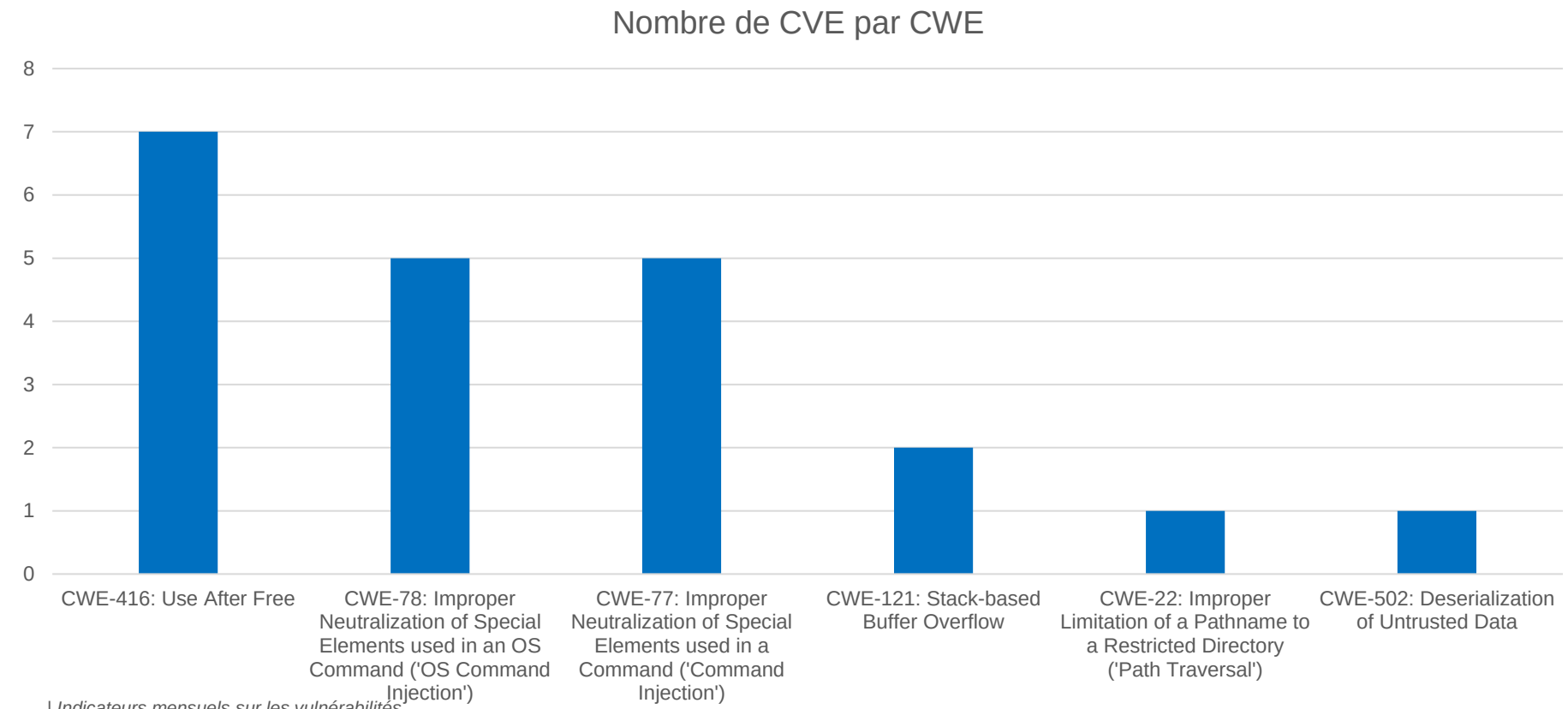
Les routeurs, les systèmes d'exploitation, les solutions de sécurité systèmes et les navigateurs internet sont les principaux types d'équipements affectés par les vulnérabilités publiées.



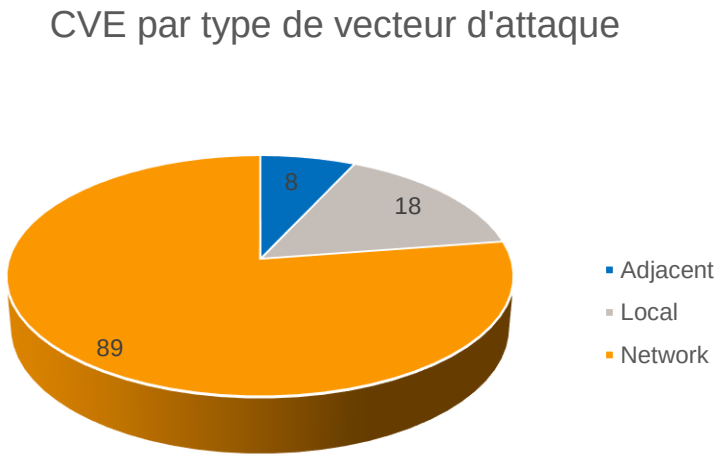
Types de menaces

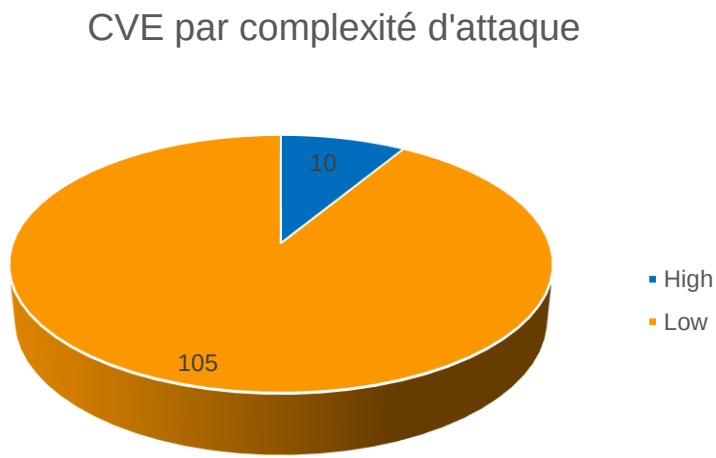


TOP 6 des failles selon le référentiel CWE



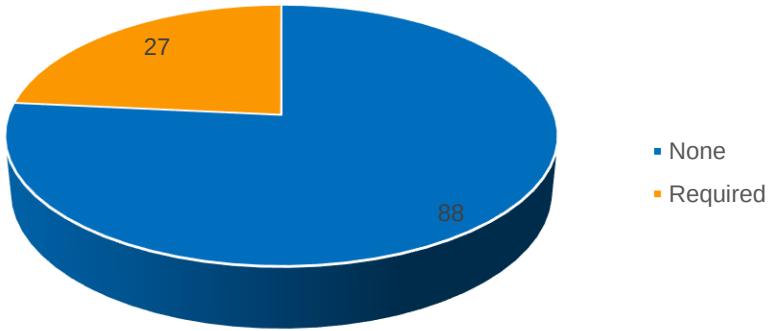
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



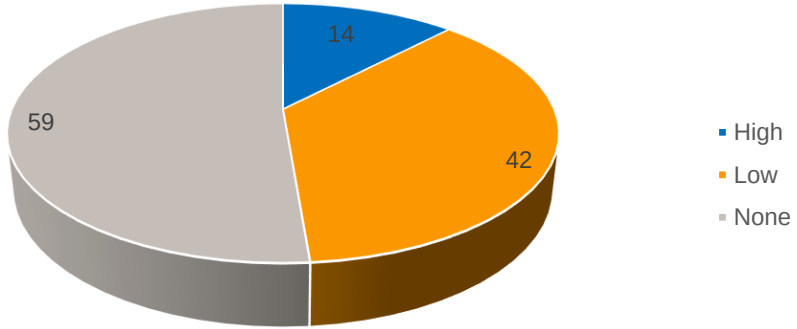


Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

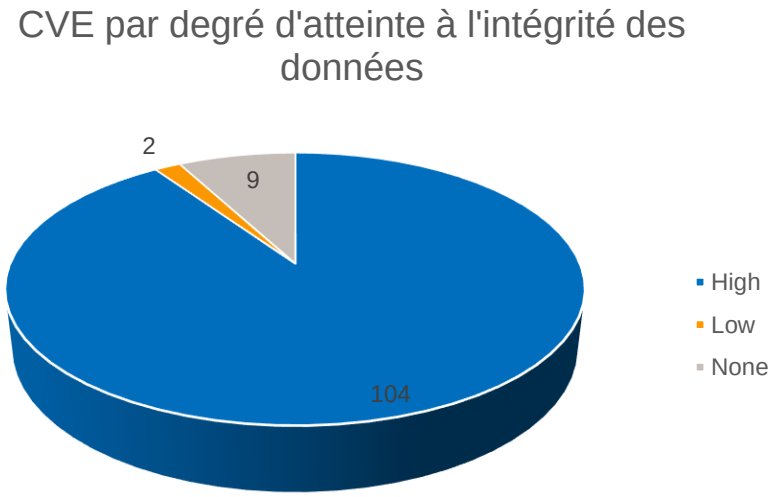
CVE par interaction utilisateur

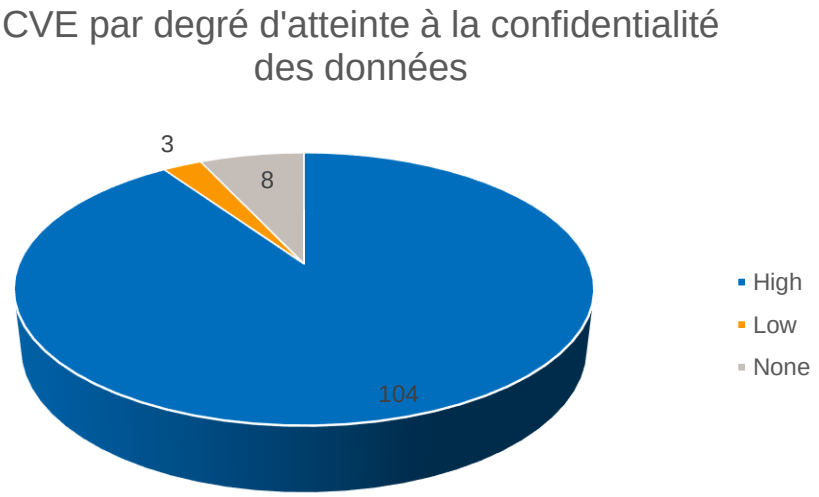


CVE par type de privilèges requis

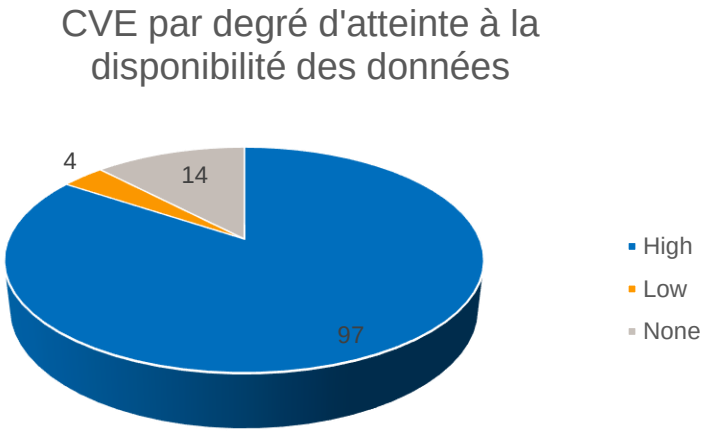


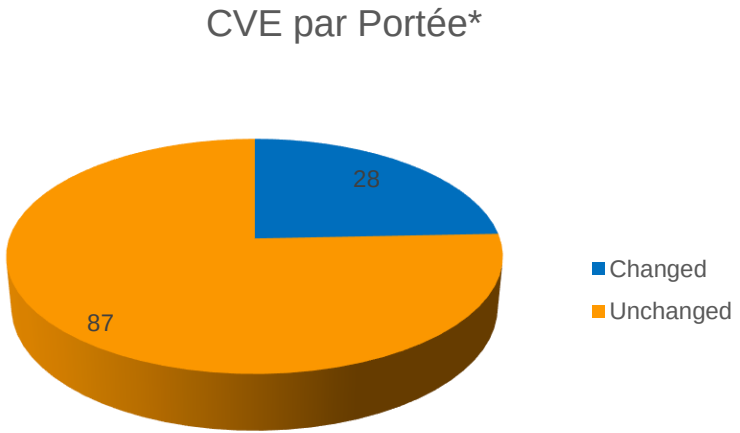
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données





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.