CERT Santé

LA E-SANTÉ FRANÇAISE

AGENCE DU NUMÉRIQUE EN SANTÉ

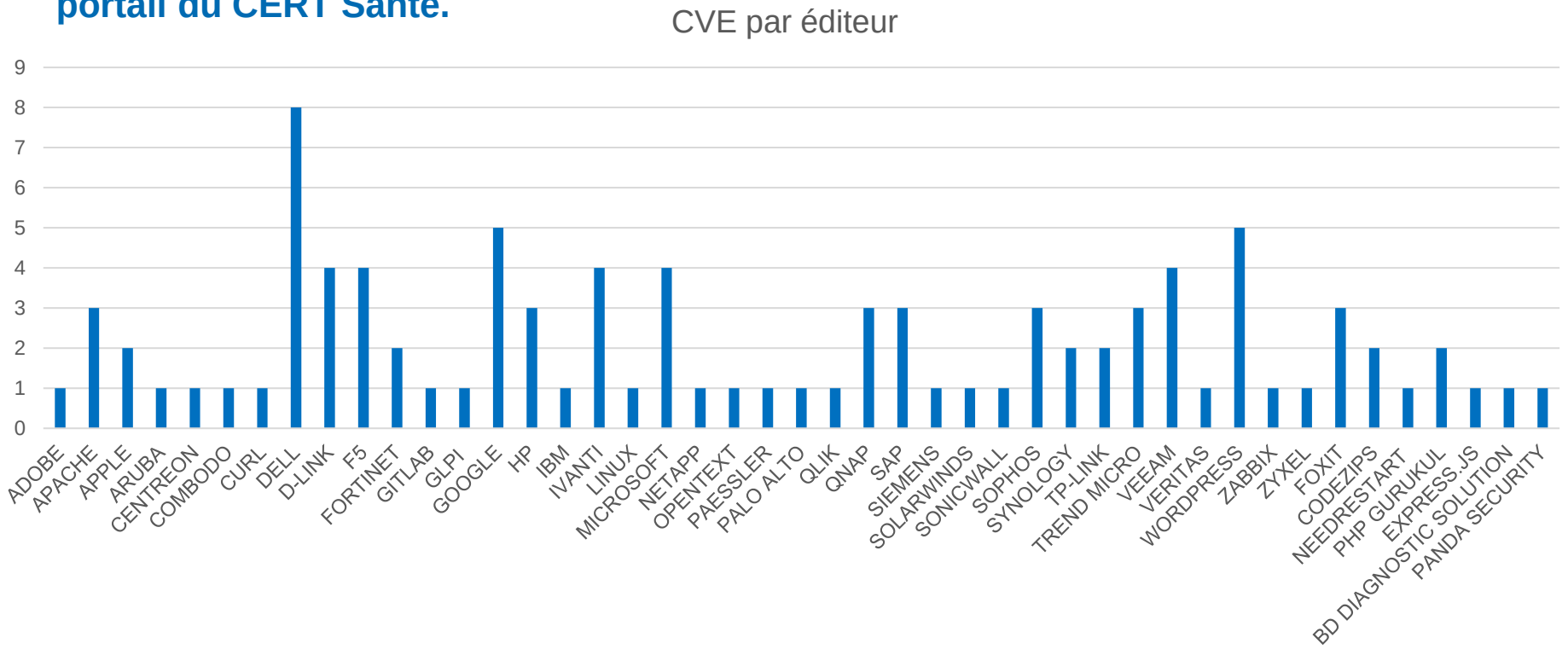
La transformation commence ici

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

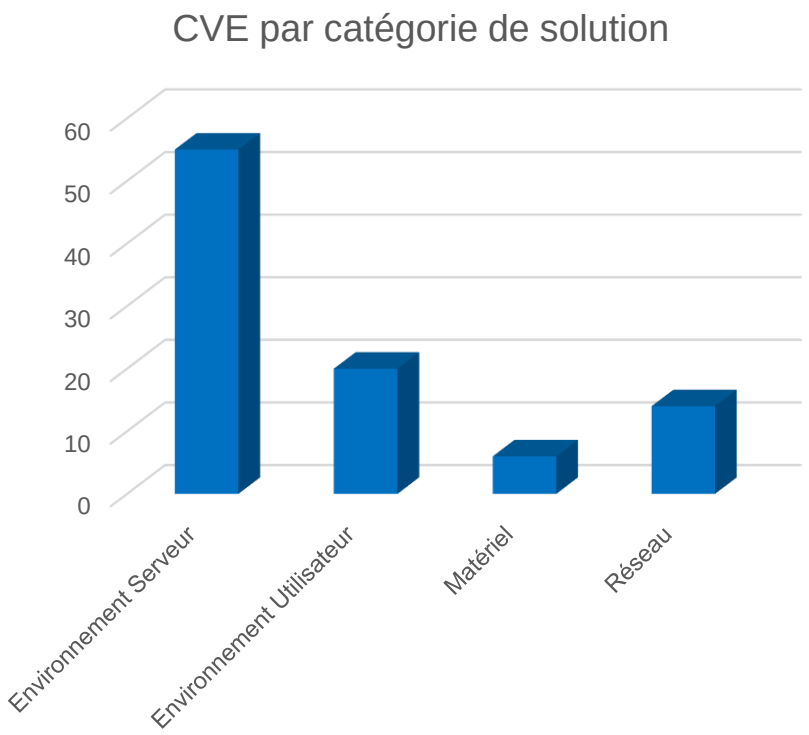
Janvier 2025

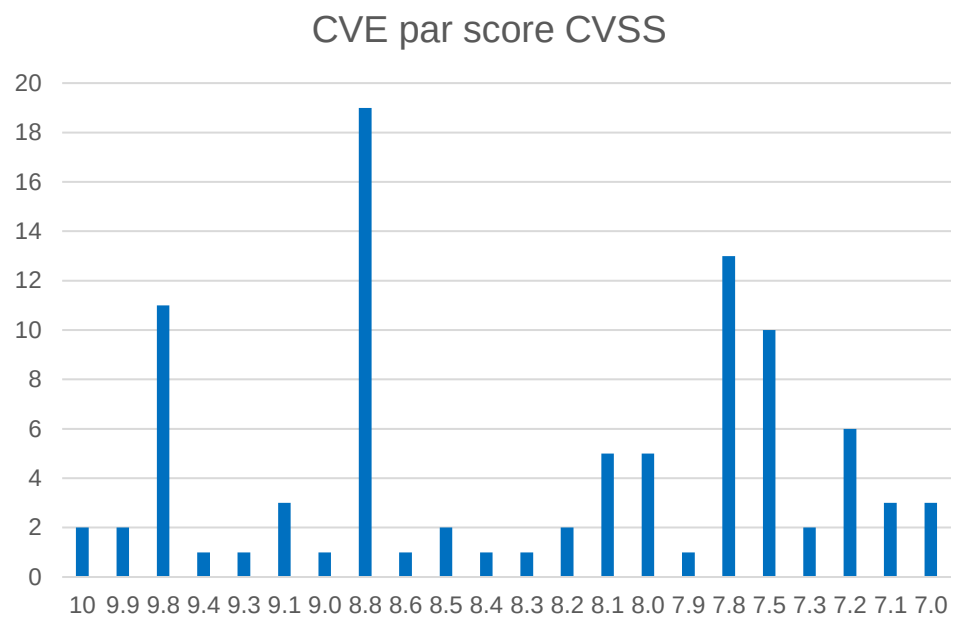
Nombre de CVE par éditeur

95 vulnérabilités ont été analysées et publiées (parmi lesquelles 3 alertes) sur le portail du CERT Santé.

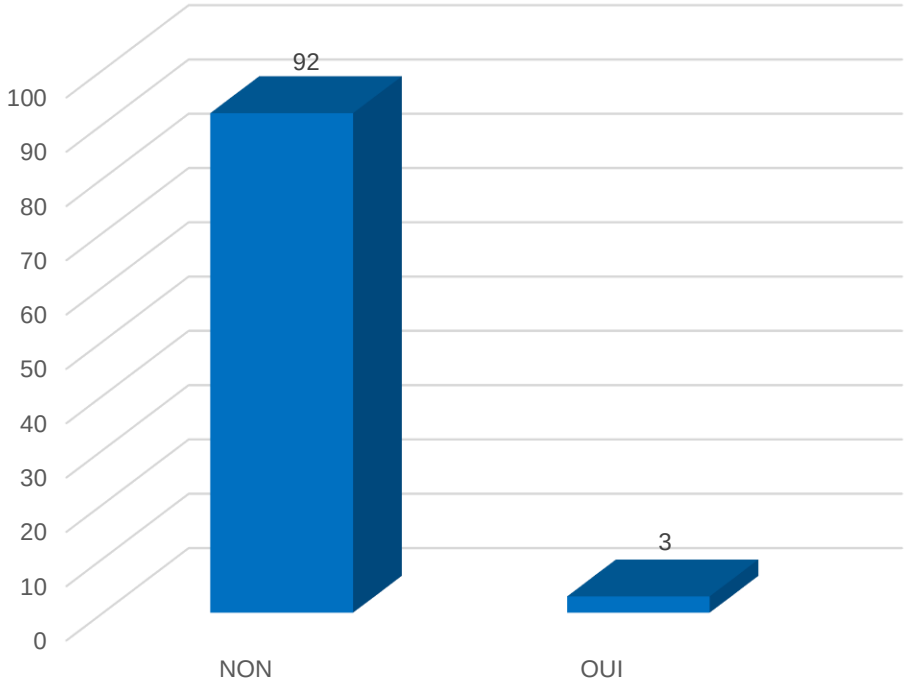


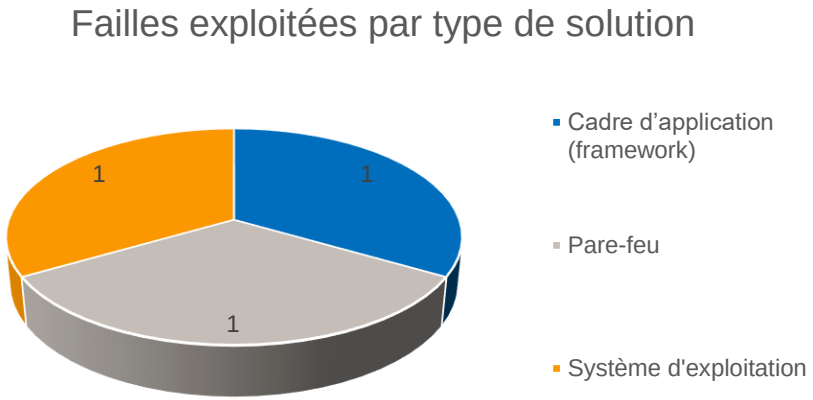
Nombre de CVE par catégorie de produit et score CVSS

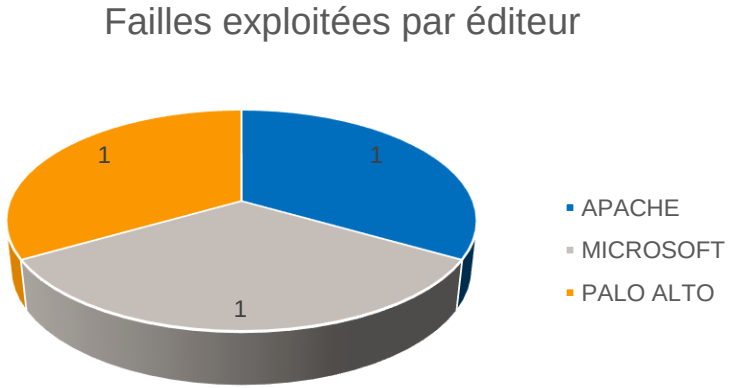




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

7.8

Microsoft

Élévation de privilèges | Exploitée

(CVE-2024-49138)

Un défaut de gestion de la mémoire dans le pilote Windows *Common Log File System* (CLFS) permet à un attaquant authentifié d'obtenir les privilèges *SYSTEM*.

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

9.8

Fortinet

Contournement de la politique de sécurité | Preuve de Concept

(CVE-2023-34990)

Un défaut de traversée de répertoires dans Fortinet FortiWLM permet à un attaquant non authentifié, en envoyant des requêtes Web spécifiquement forgées, de contourner la politique de sécurité et de se procurer un jeton de session admin.

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

7.5

Palo Alto

Déni de Service | Exploitée

(CVE-2024-3393)

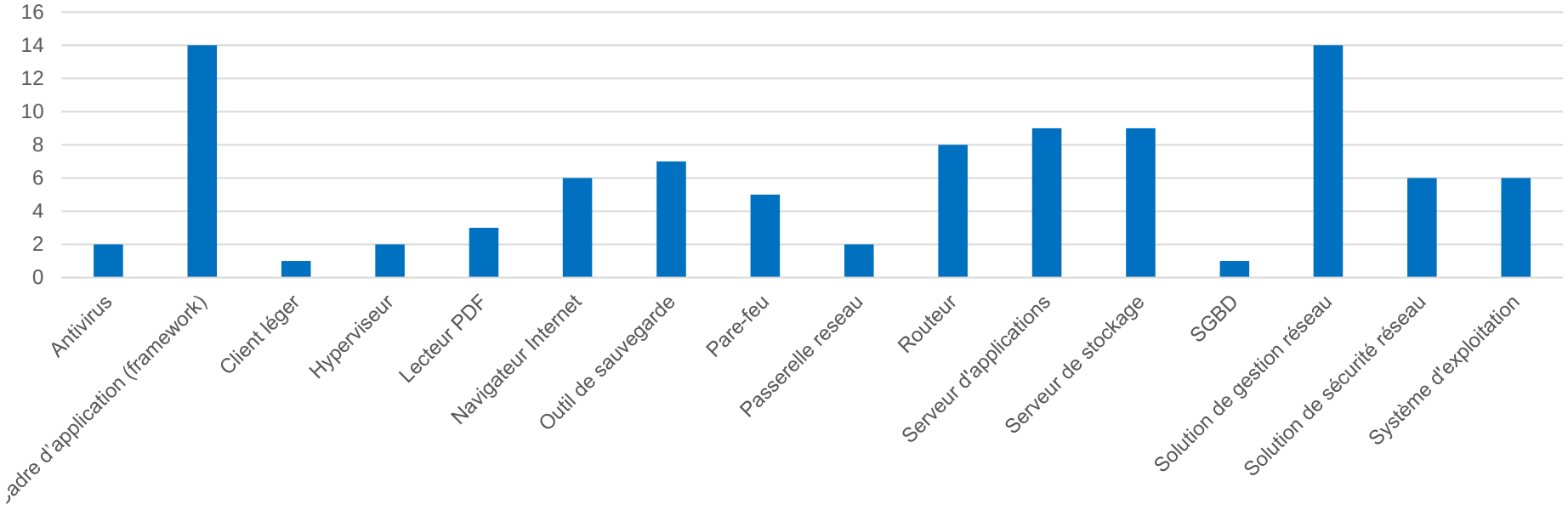
Un défaut dans la fonctionnalité de sécurité DNS de Palo Alto PAN-OS permet à un attaquant non authentifié, en envoyant des paquets spécifiquement forgés, de provoquer un déni de service. L'exploitation successive de la faille entraîne le passage en mode maintenance de l'équipement.

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

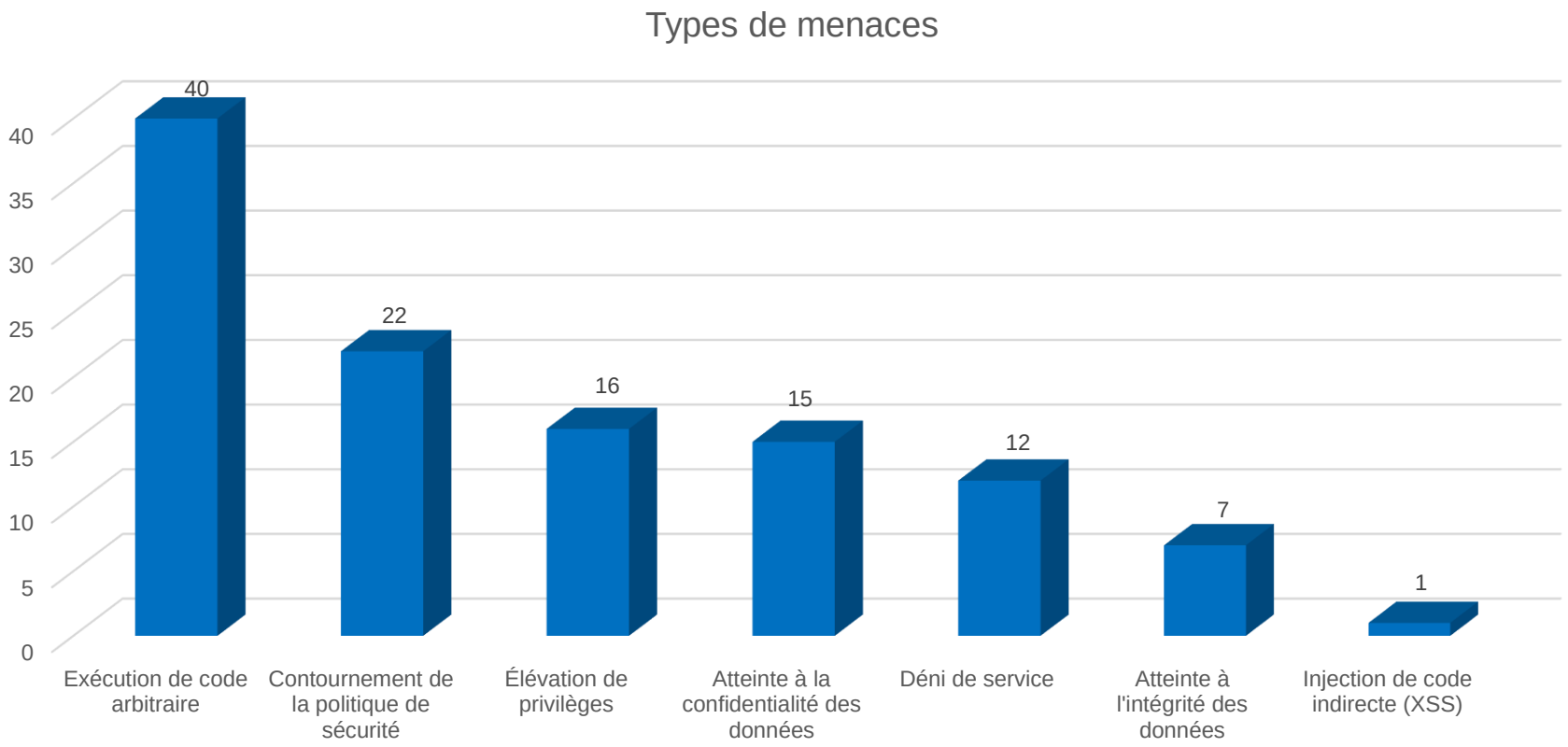
Types de solutions vulnérables

Les cadres d'applications, les solutions de gestion réseau, les serveurs d'applications et les serveurs de stockage sont les principaux types d'équipements affectés par les vulnérabilités publiées.

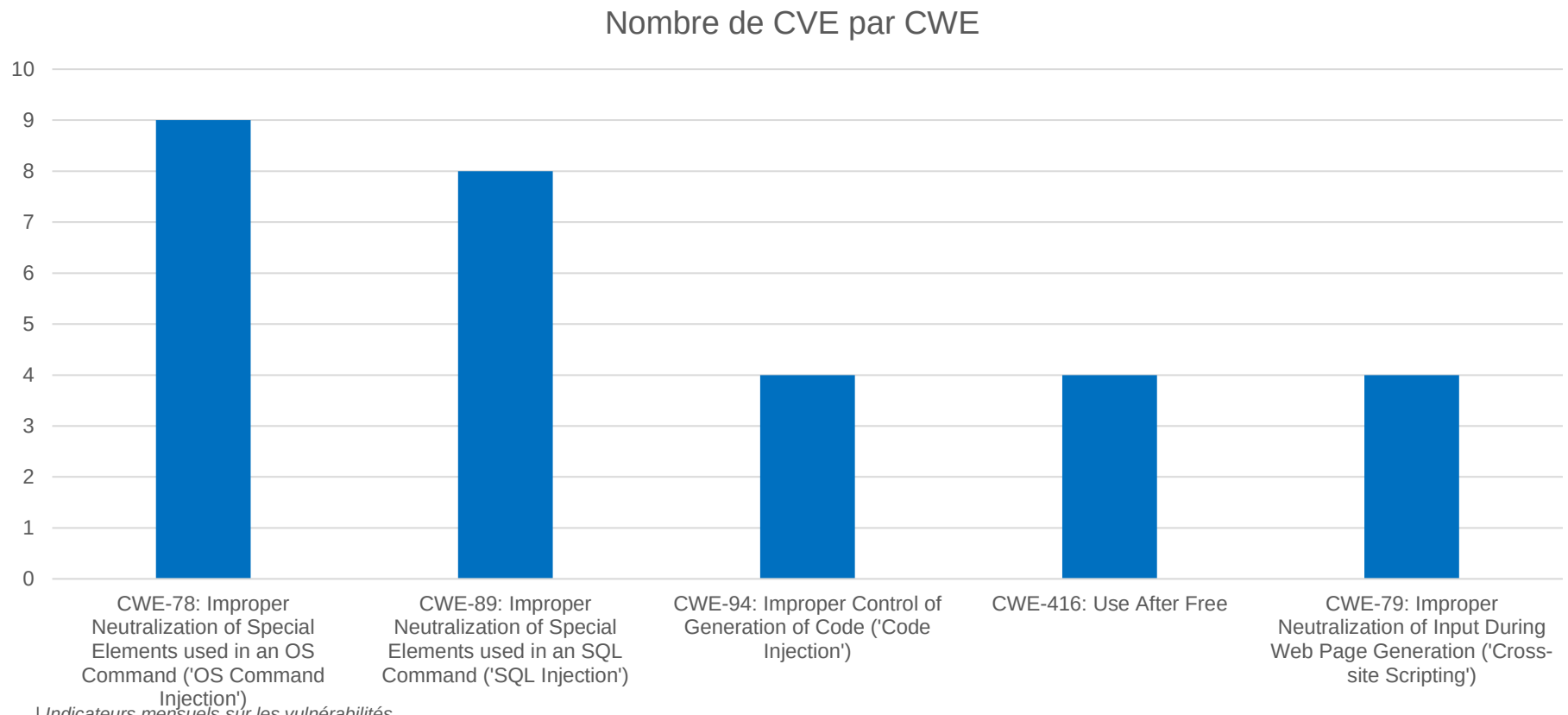
CVE par type de solution



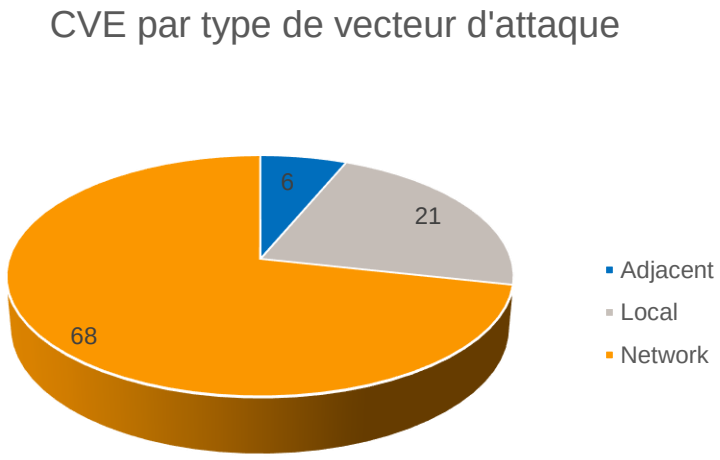
Types de menaces

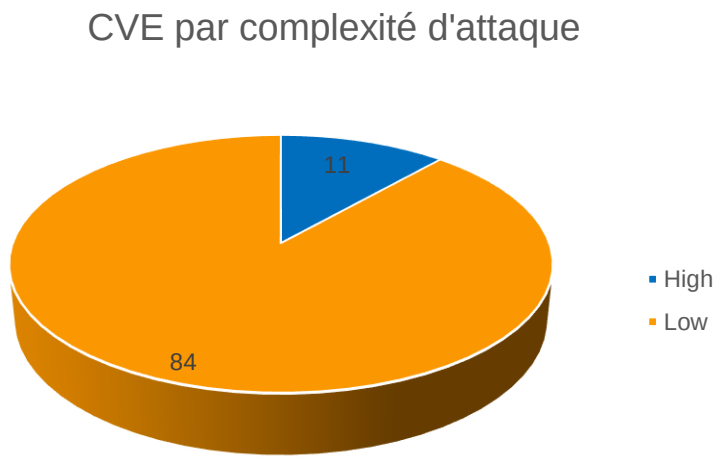


TOP 5 des failles selon le référentiel CWE



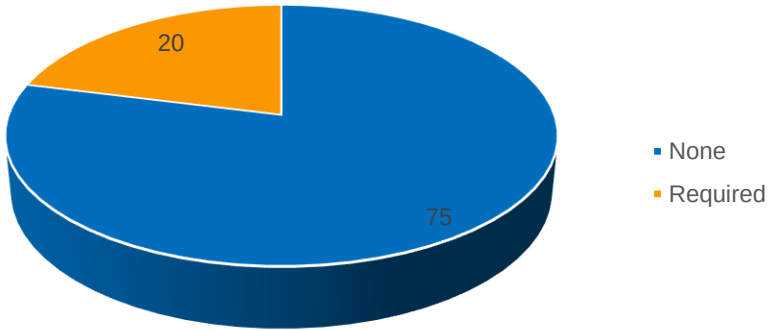
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



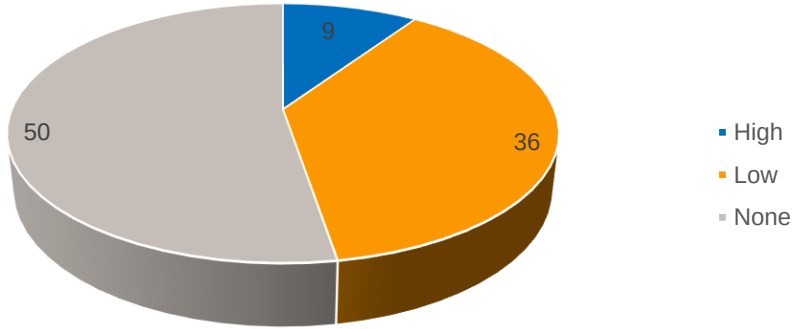


Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

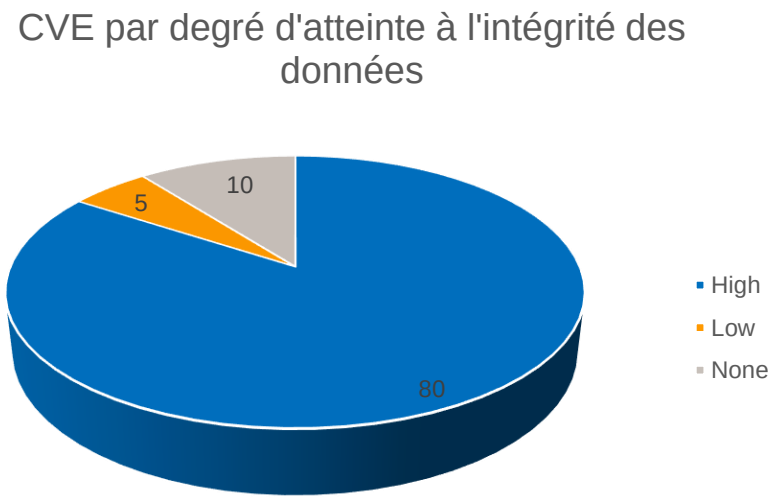
CVE par interaction utilisateur

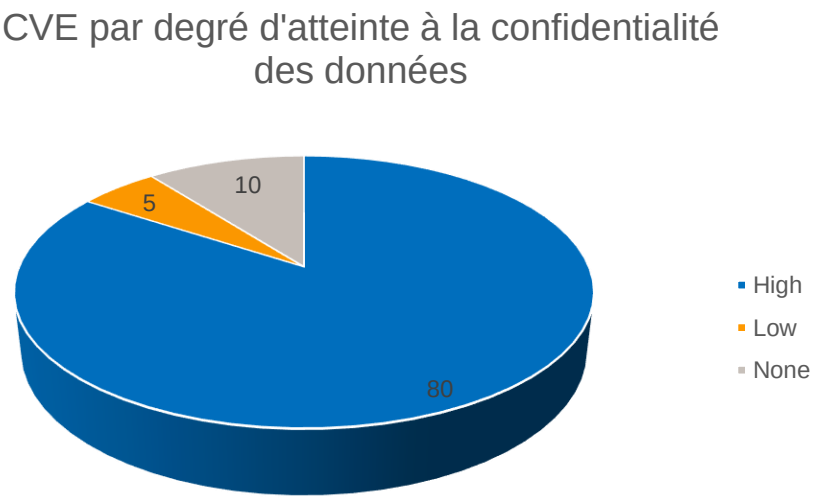


CVE par type de privilèges requis

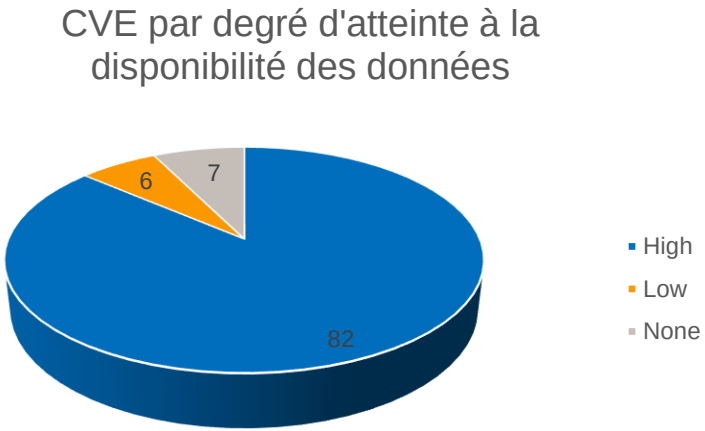


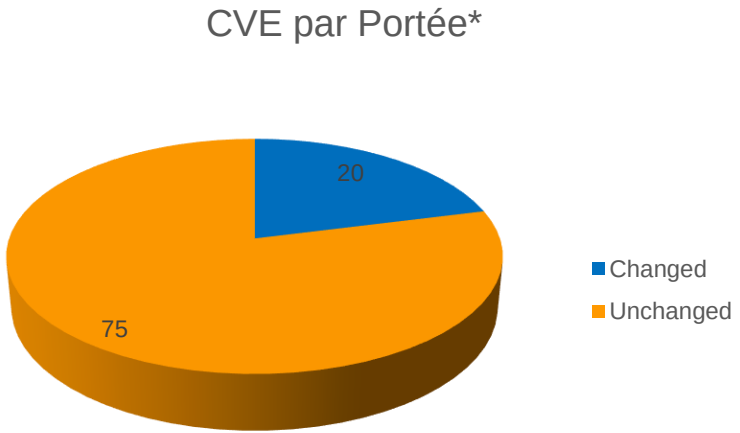
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données





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.