CERT Santé

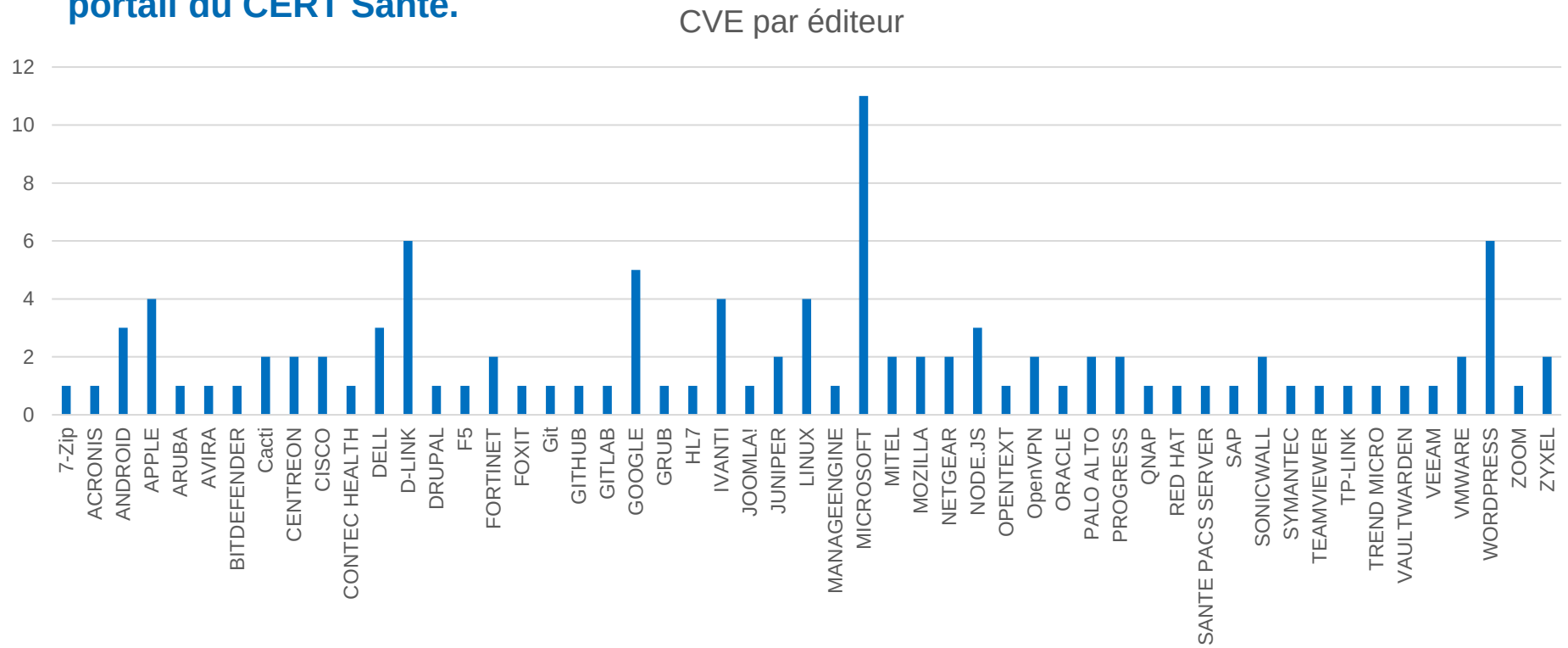
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Indicateurs sur la publication des CVE pour le mois de janvier 2025

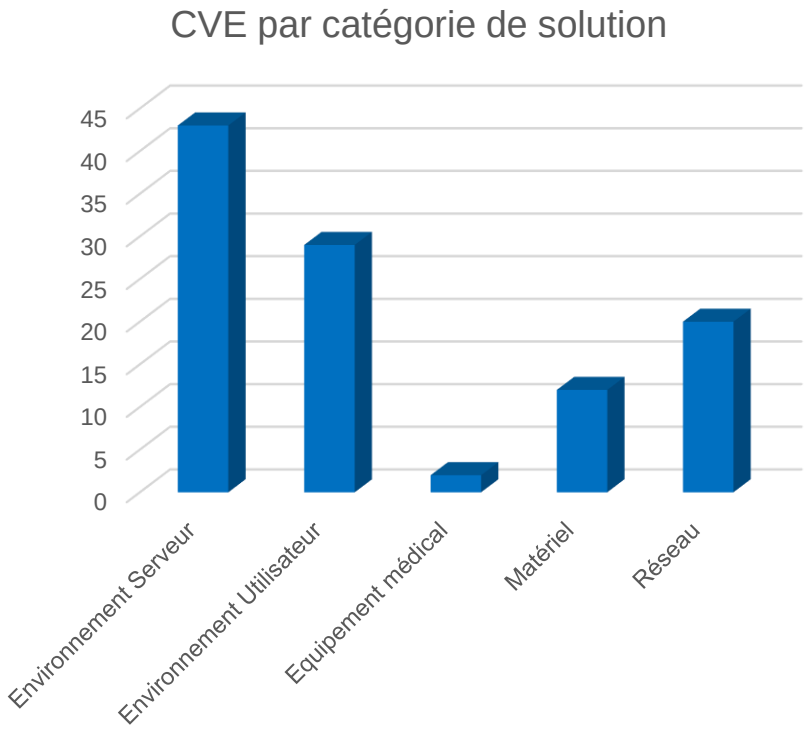
Février 2025

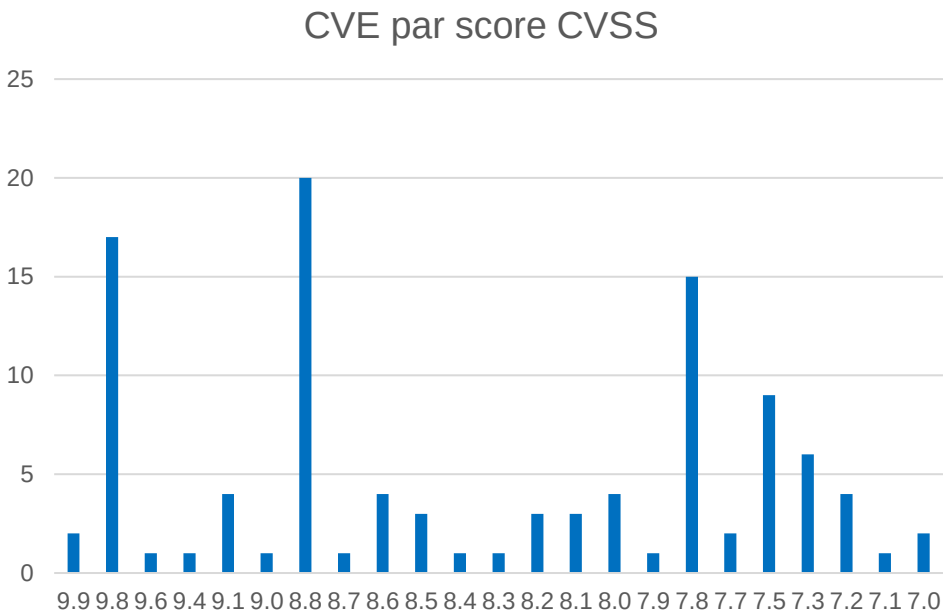
Nombre de CVE par éditeur

106 vulnérabilités ont été analysées et publiées (parmi lesquelles 10 alertes) sur le portail du CERT Santé.



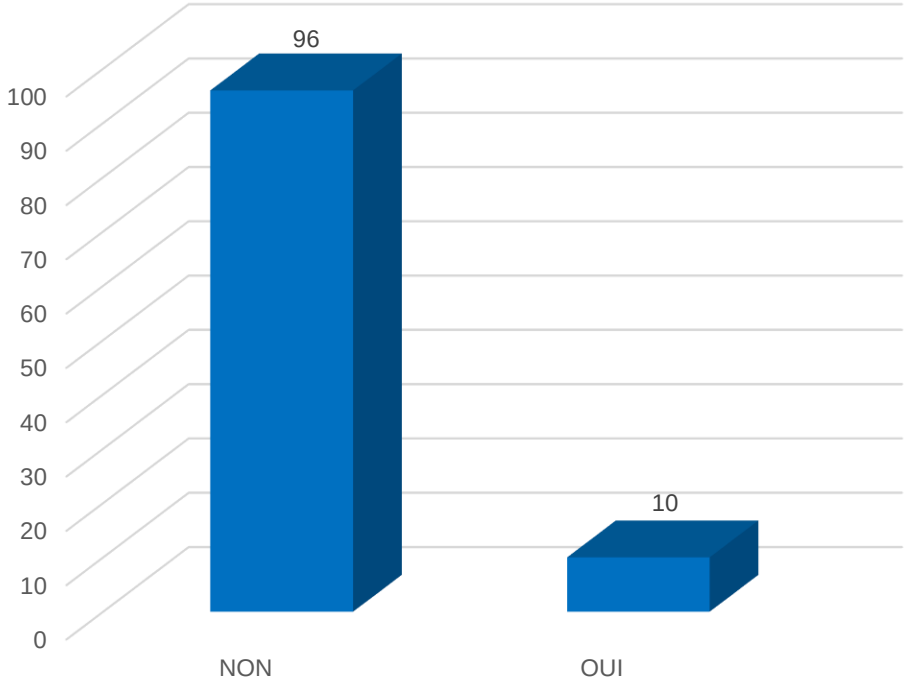
Nombre de CVE par catégorie de produit et score CVSS



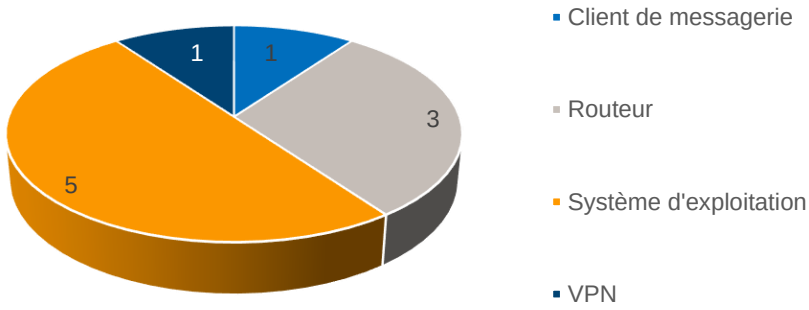


Vulnérabilités exploitées

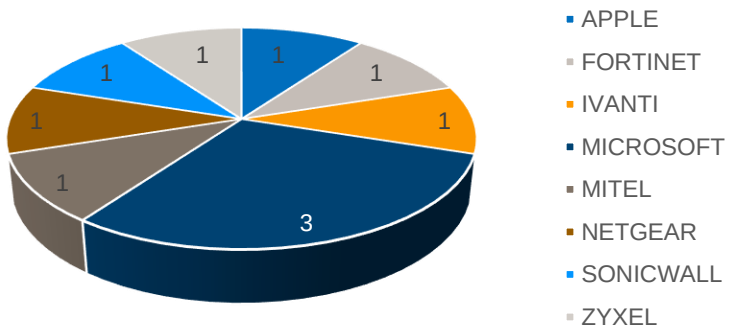
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

Fortinet

(CVE-2024-55591)

Exécution de code arbitraire

Exploitée

Un contournement de l'authentification dans Fortinet FortiOS et FortiProxy permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées au module websocket Node.js, d'obtenir des privilèges super-admin et d'exécuter du code arbitraire.

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

Ivanti

(CVE-2025-0282)

Exécution de code arbitraire

Exploitée

Un défaut de contrôle de la mémoire dans les produits Ivanti Connect Secure, Policy Secure et Neurons for ZTA gateways permet à un attaquant non authentifié d'exécuter du code arbitraire.

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

7-Zip

(CVE-2025-0411)

Exécution de code arbitraire

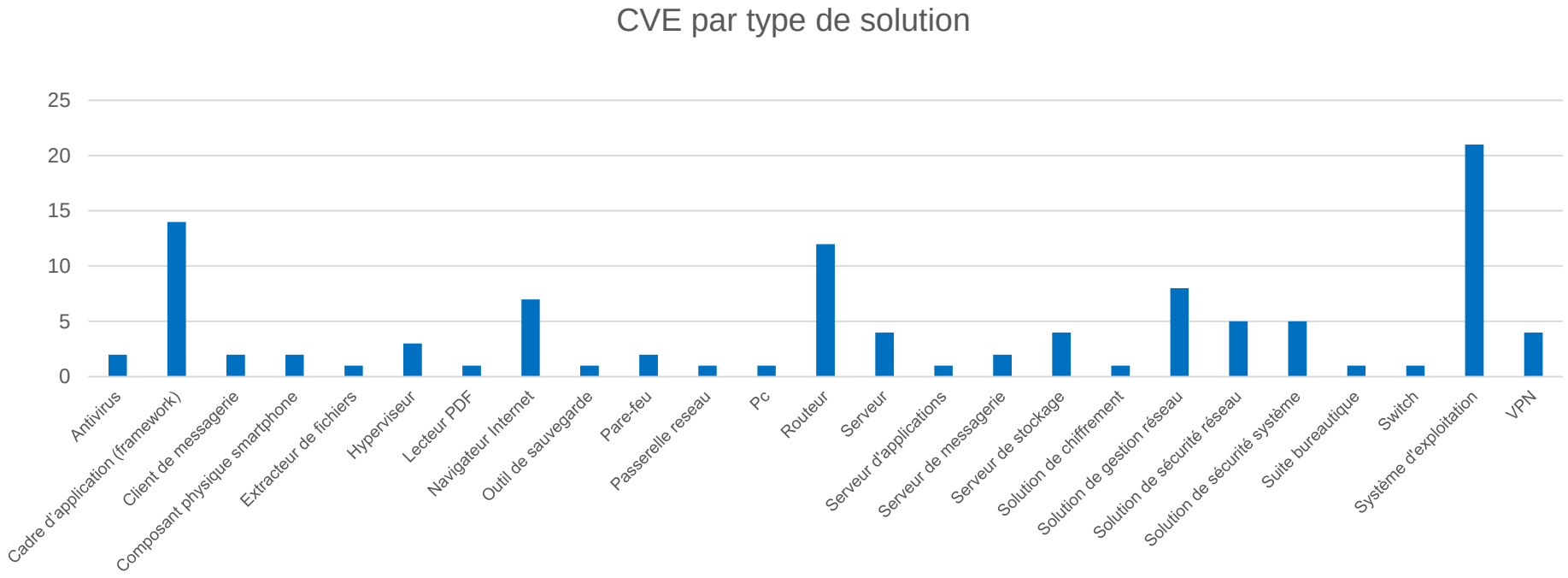
Exploitée

Un défaut dans la fonctionnalité *Mark-of-the-Web* dans 7-Zip permet à un attaquant non authentifié, en persuadant une victime d'ouvrir une archive spécifiquement forgée, d'exécuter du code arbitraire à distance.

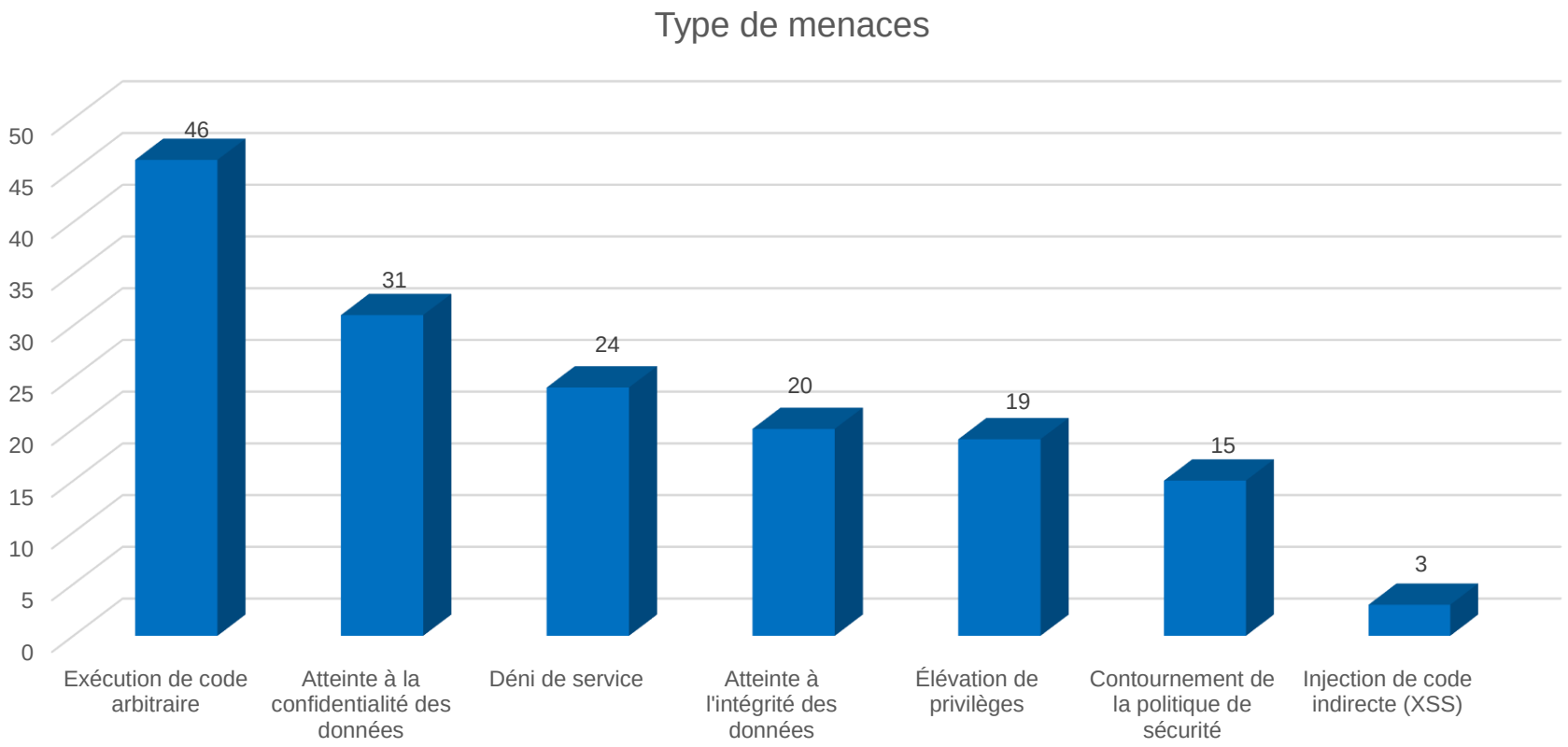
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

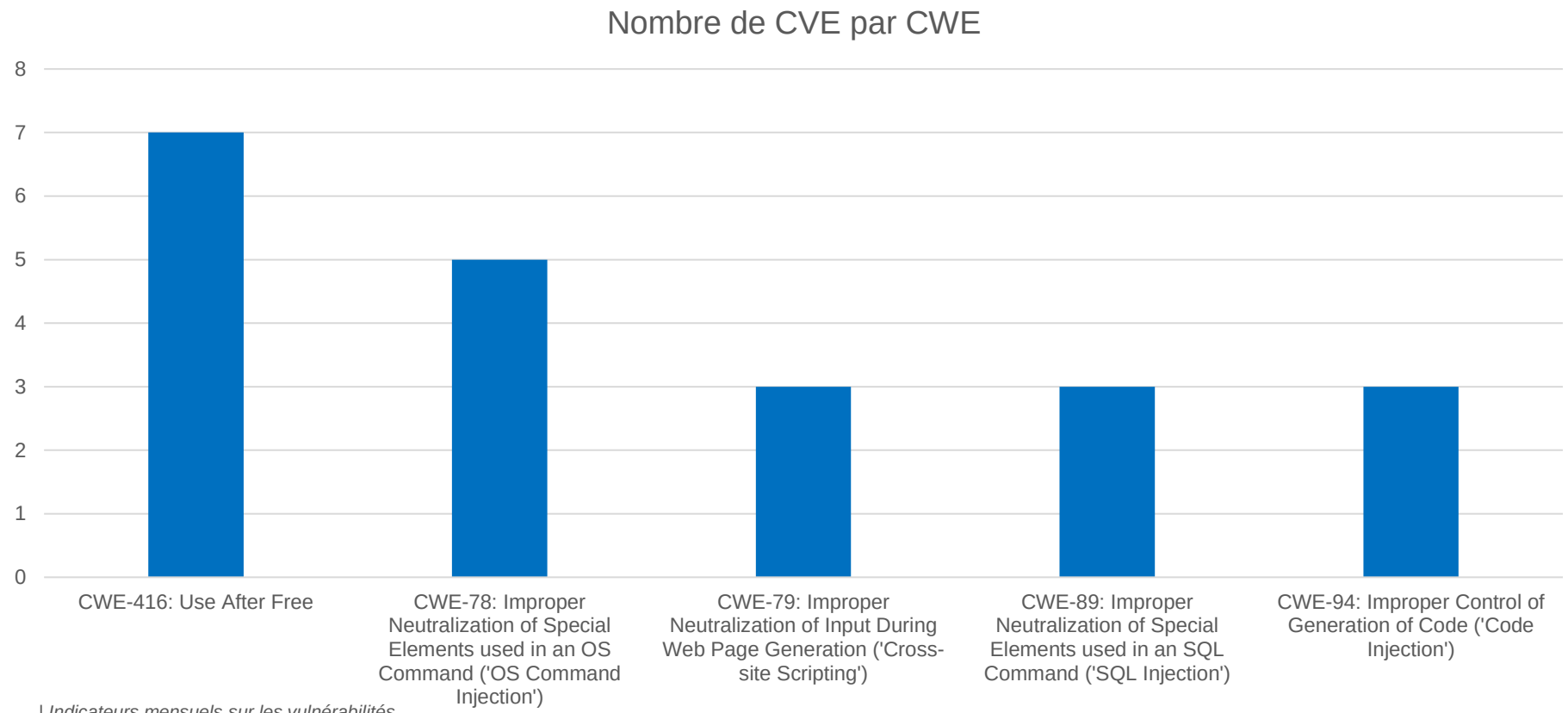
Les systèmes d'exploitation, les cadres d'application et les routeurs sont les principaux types d'équipements affectés par les vulnérabilités publiées.



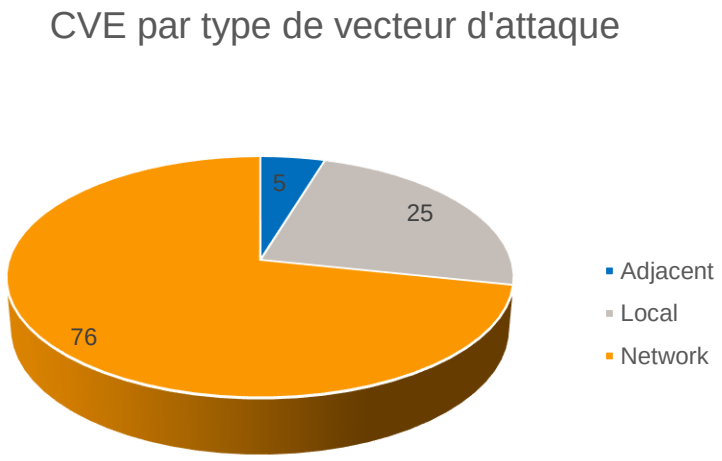
Types de menaces

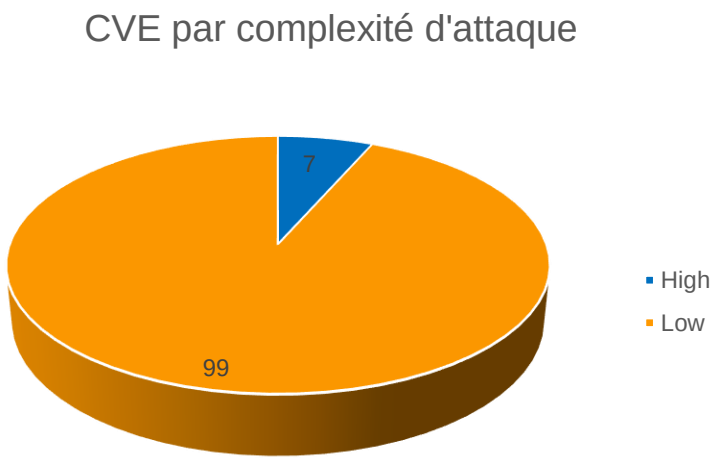


TOP 5 des failles selon le référentiel CWE



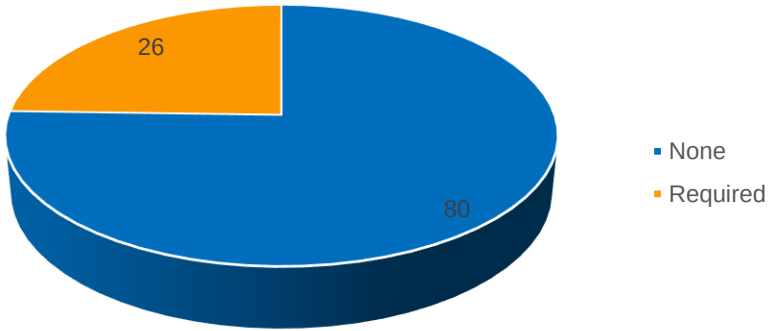
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



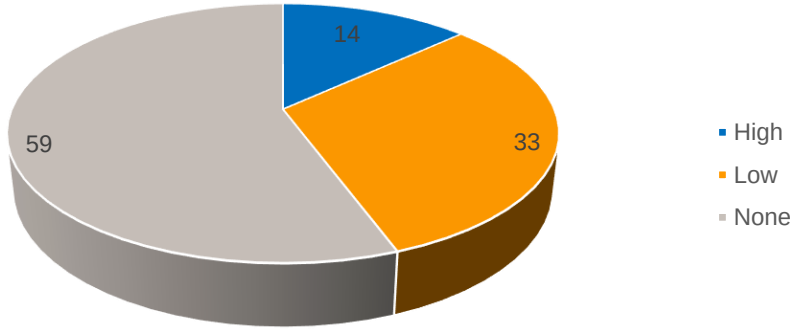


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

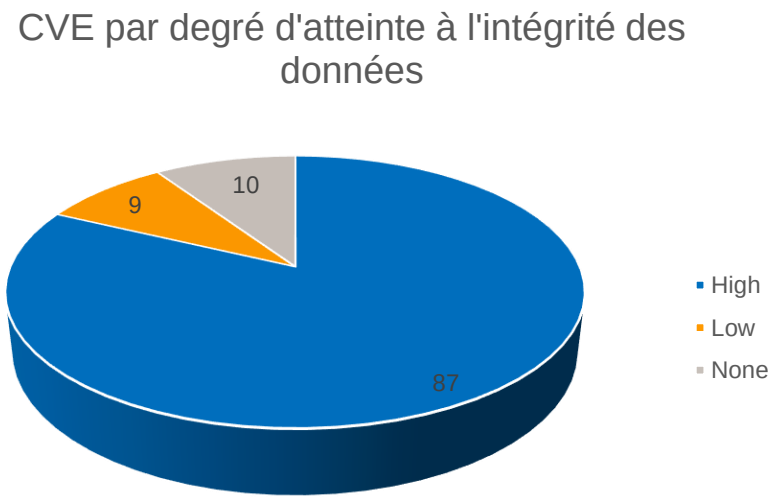
CVE par interaction utilisateur

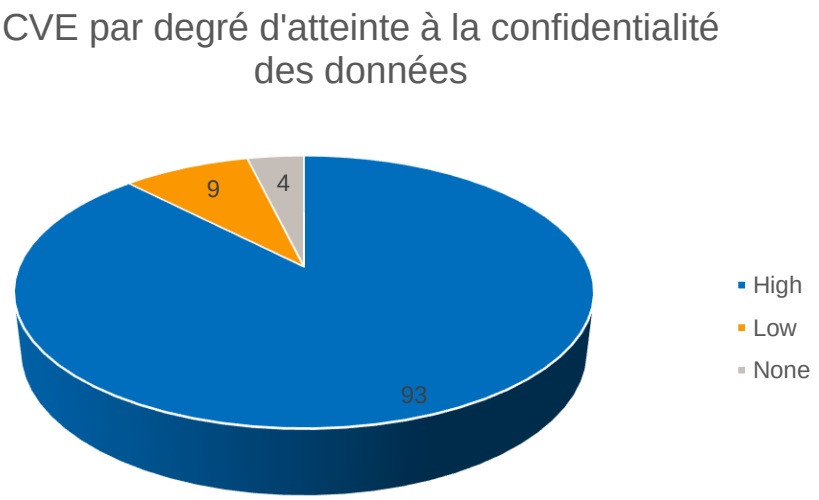


CVE par type de privilèges requis

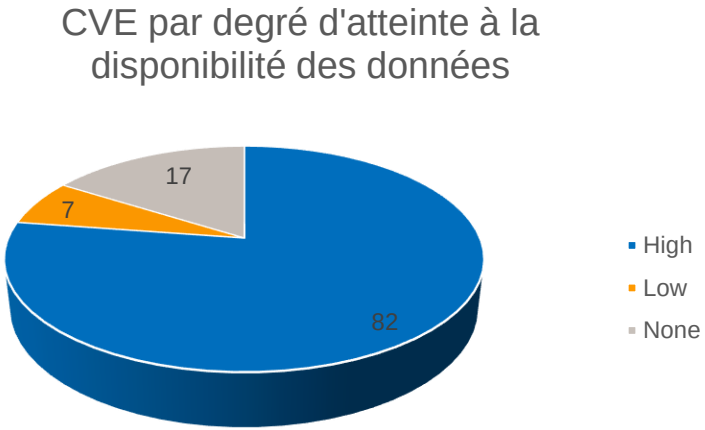


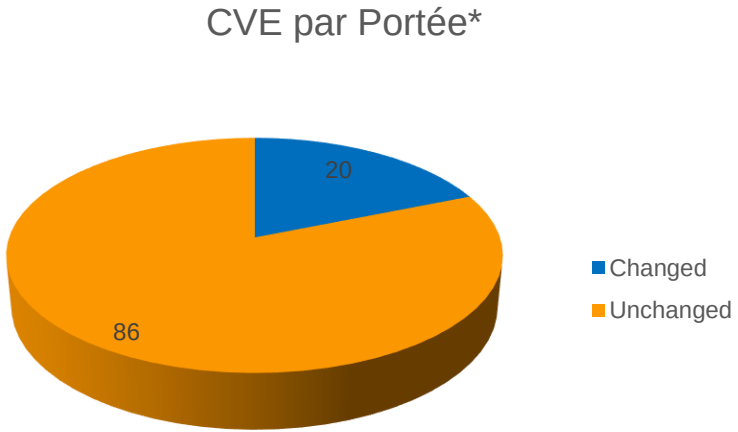
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données





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.