CERT Santé

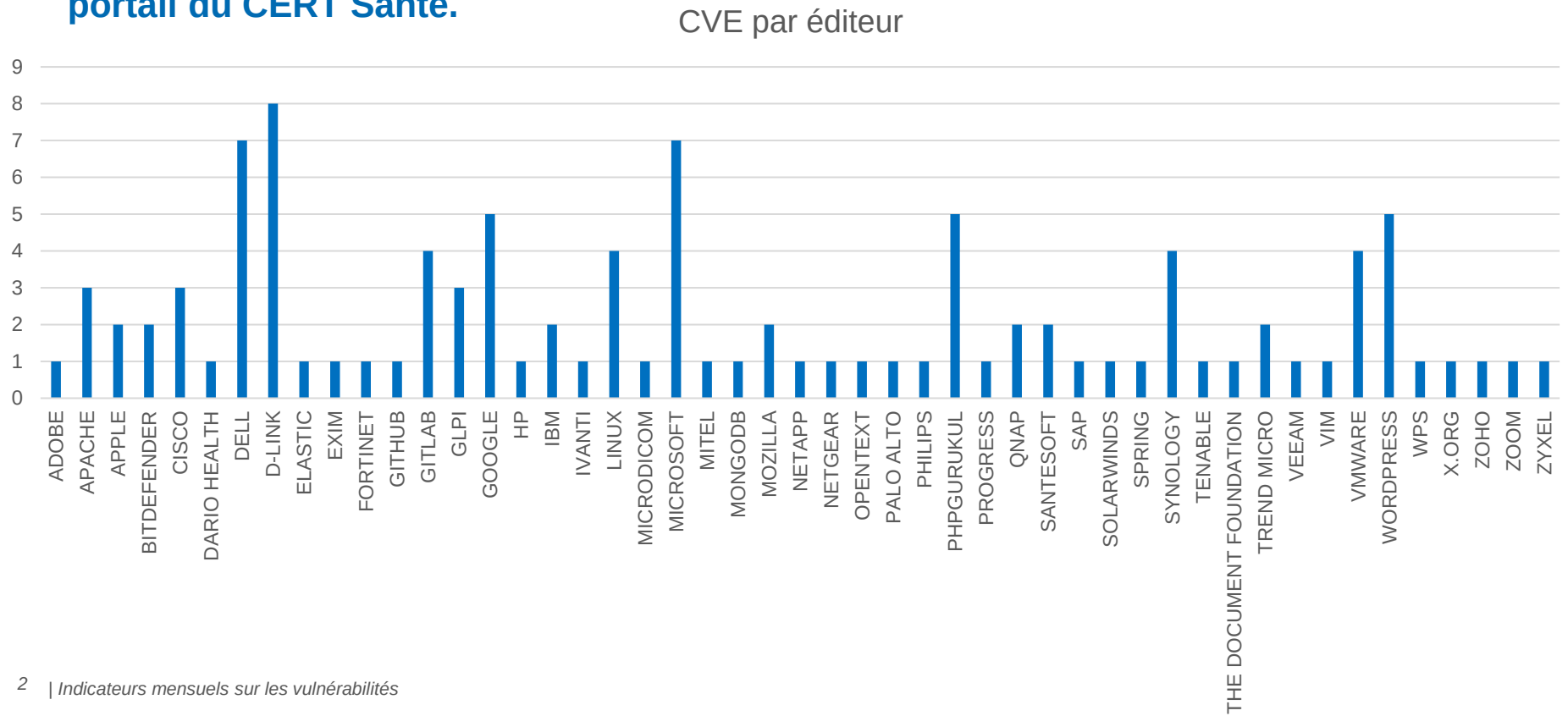
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

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

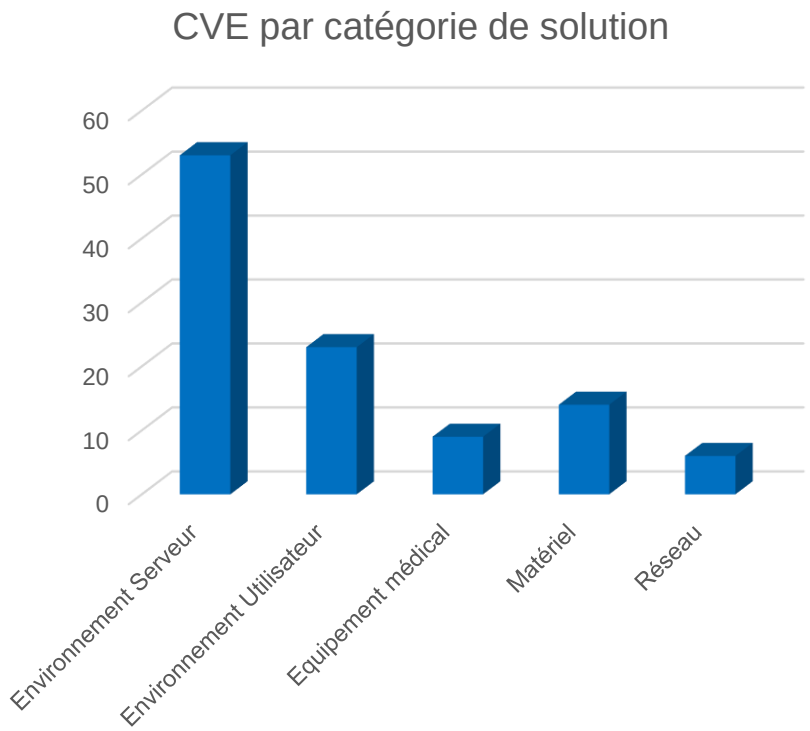
Avril 2025

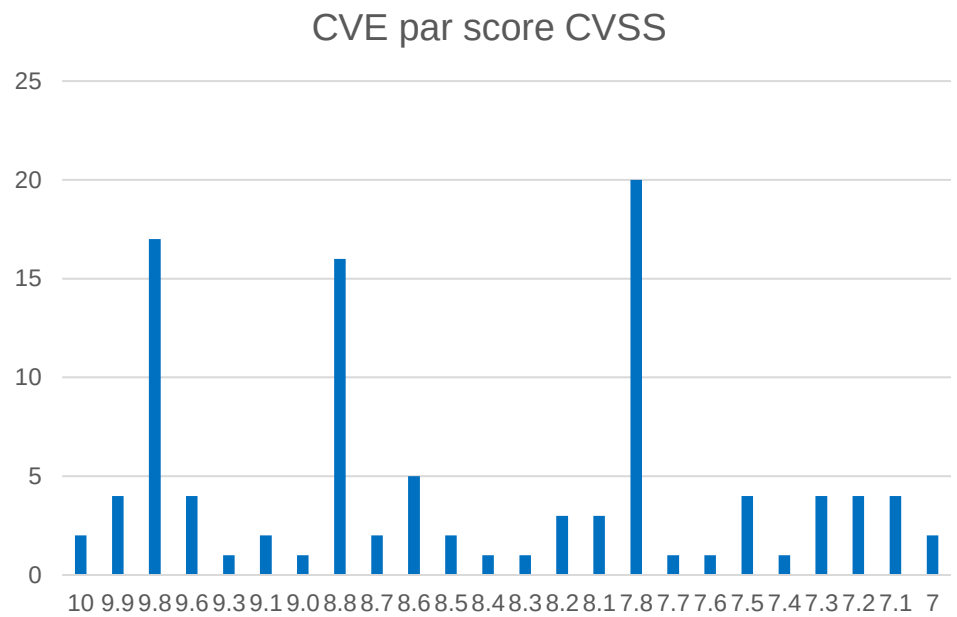
Nombre de CVE par éditeur

105 vulnérabilités ont été analysées et publiées (parmi lesquelles 16 alertes) sur le portail du CERT Santé.



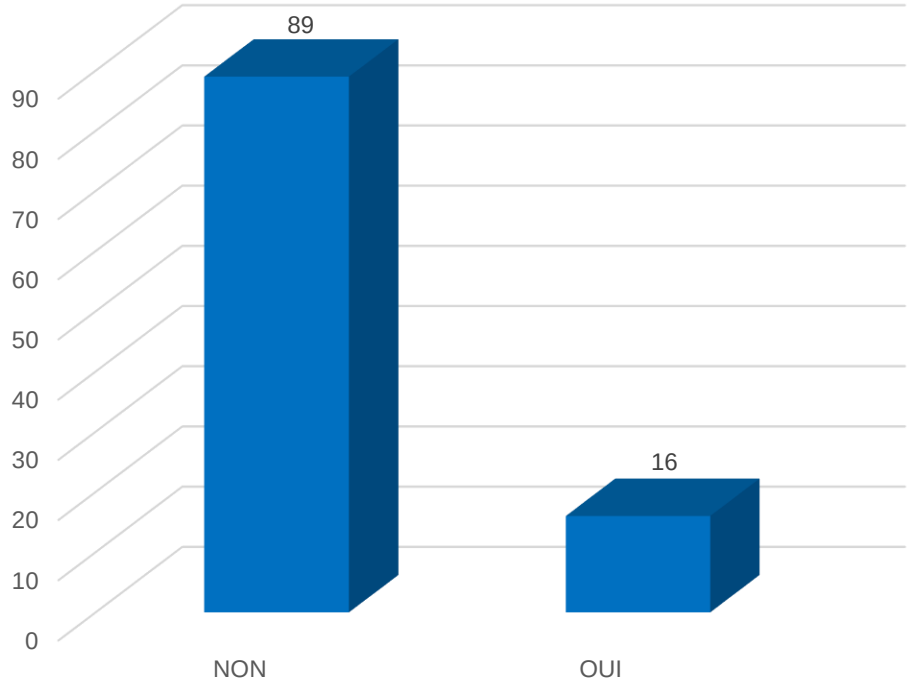
Nombre de CVE par catégorie de produit et score CVSS



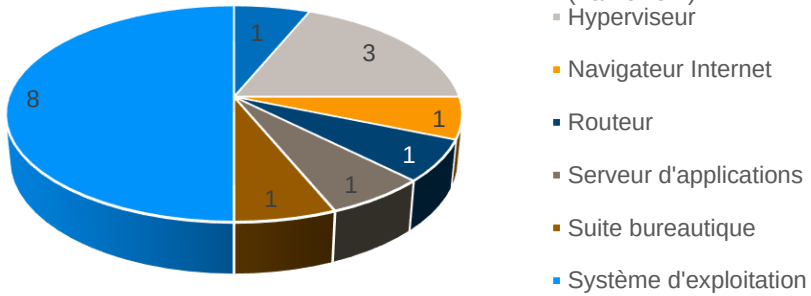


Vulnérabilités exploitées

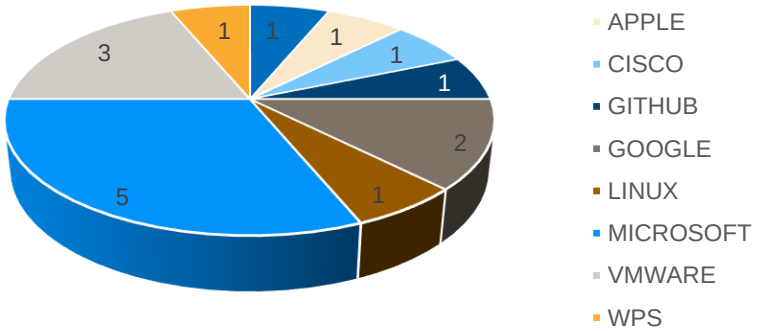
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

9.3

VMware
(CVE-2025-22224)

Exécution de code arbitraire | Exploitée

Un défaut lié à une exécution concurrente (*race condition*) dans plusieurs produits VMware permet à un attaquant, ayant un accès administrateur local sur une machine virtuelle, d'exécuter du code arbitraire sur la machine hôte.

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

8.6

Apache Tomcat
(CVE-2025-24813)

Exécution de code arbitraire | Exploitée | Preuve de Concept

Une désérialisation non sécurisée dans le composant *Partial PUT Handler* d'Apache Tomcat permet à un attaquant, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire, de consulter ou de modifier des fichiers sensibles.

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

8.6

GitHub Actions
(CVE-2025-30066)

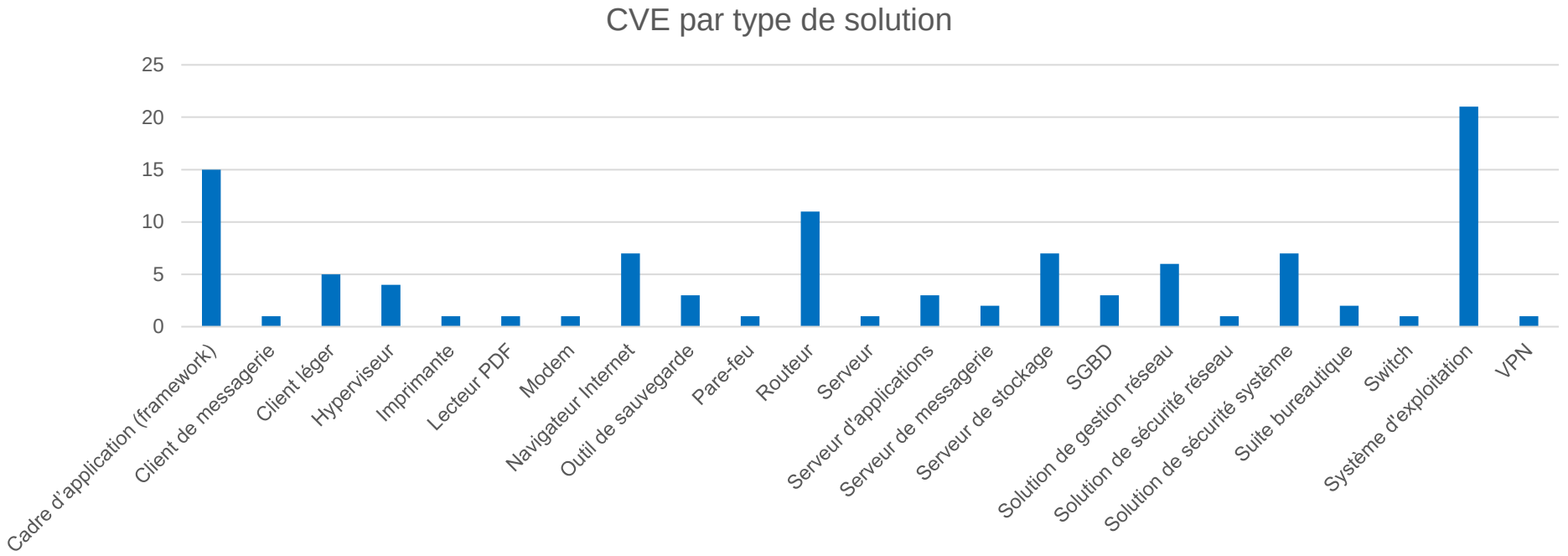
Atteinte à la confidentialité des données | Exploitée | Preuve de Concept

Du code malveillant déployé dans *tj-actions/changed-files* de GitHub Actions permet à un attaquant d'obtenir des secrets de la CI/CD (*Continuous Integration / Continuous Delivery/Deployment*).

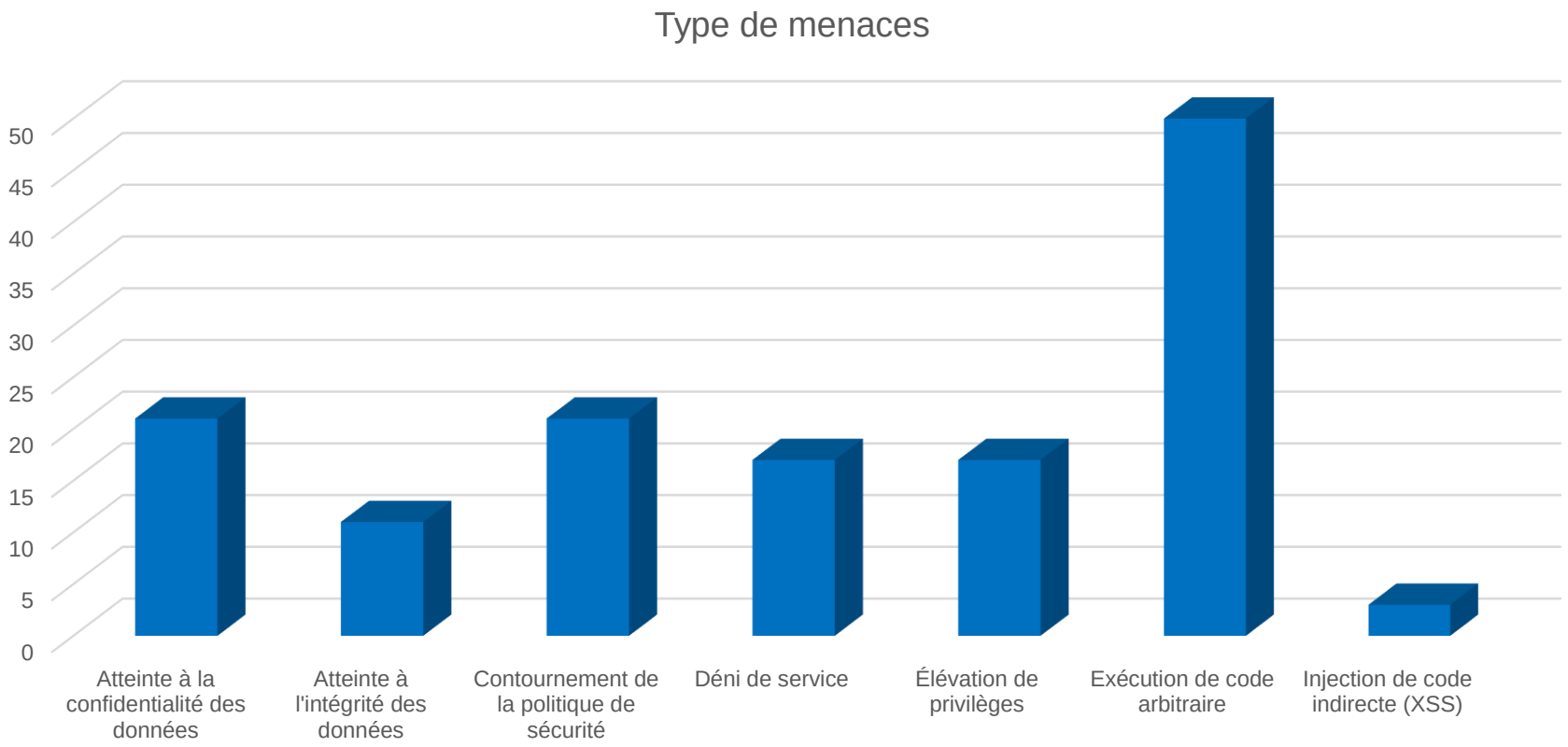
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

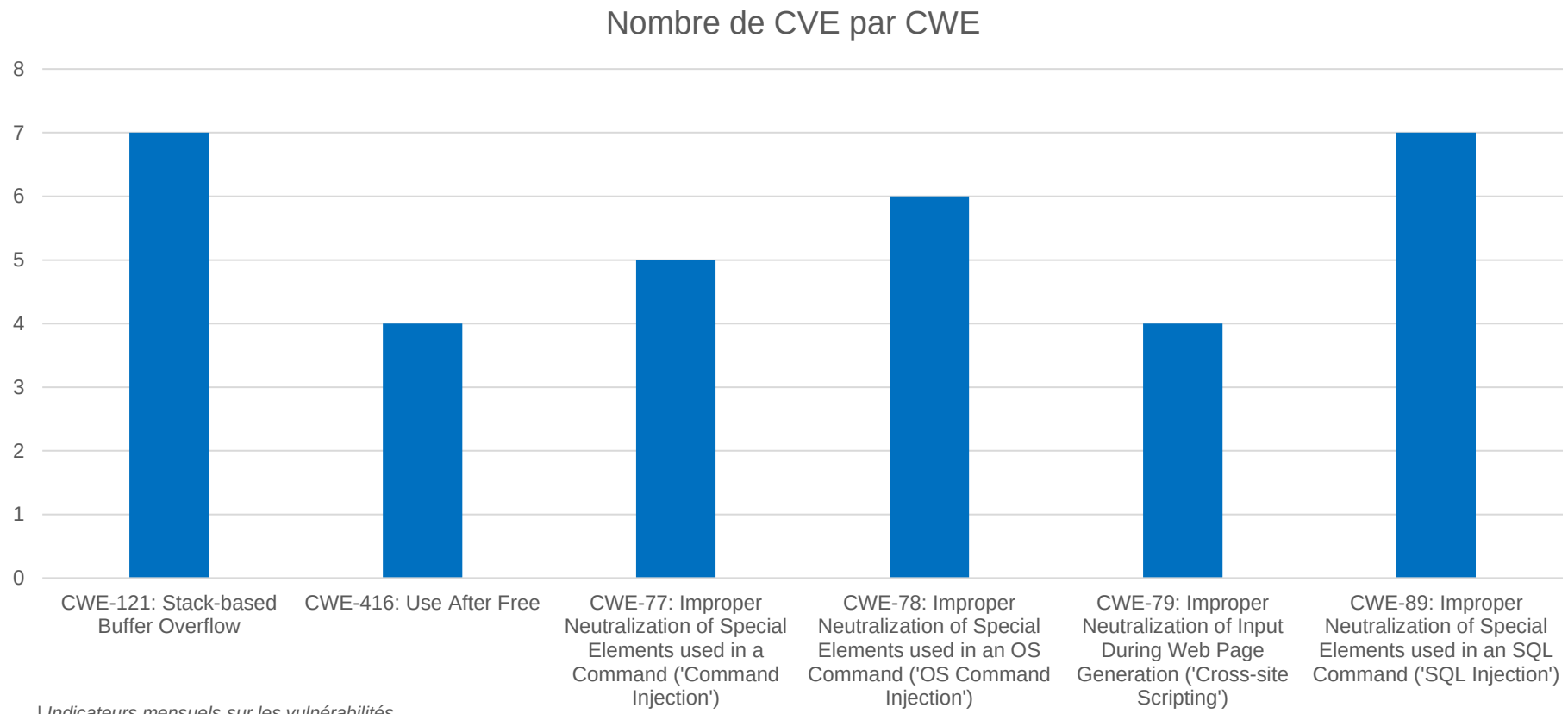
Les systèmes d'exploitation, les cadres d'application et les routeurs sont les principaux types d'équipements affectés par les vulnérabilités publiées.



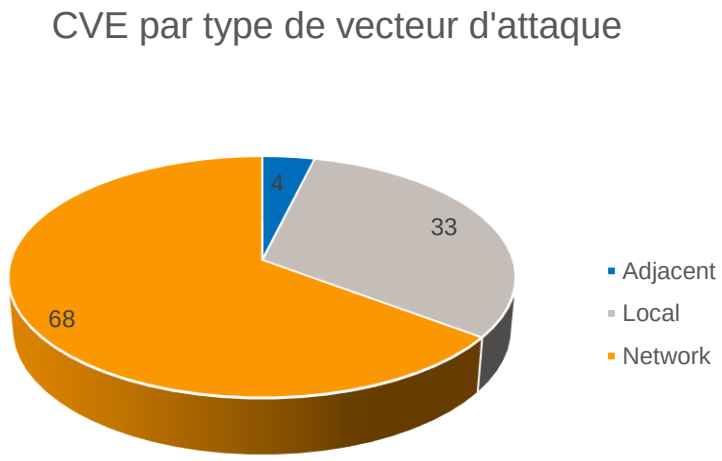
Types de menaces

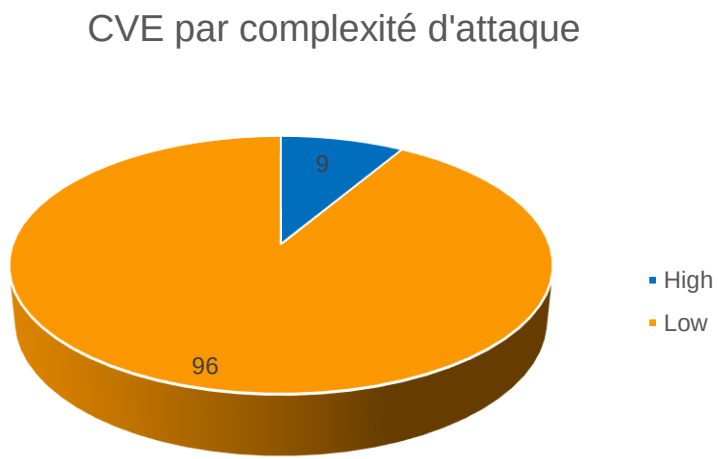


TOP 6 des failles selon le référentiel CWE



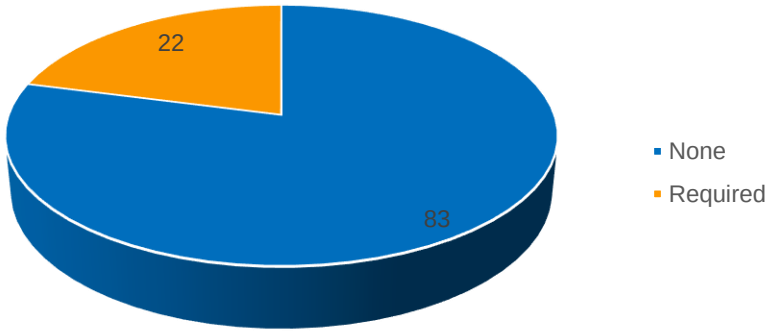
Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque



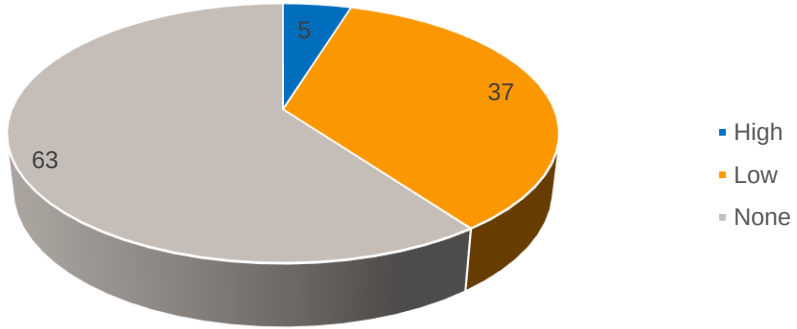


Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

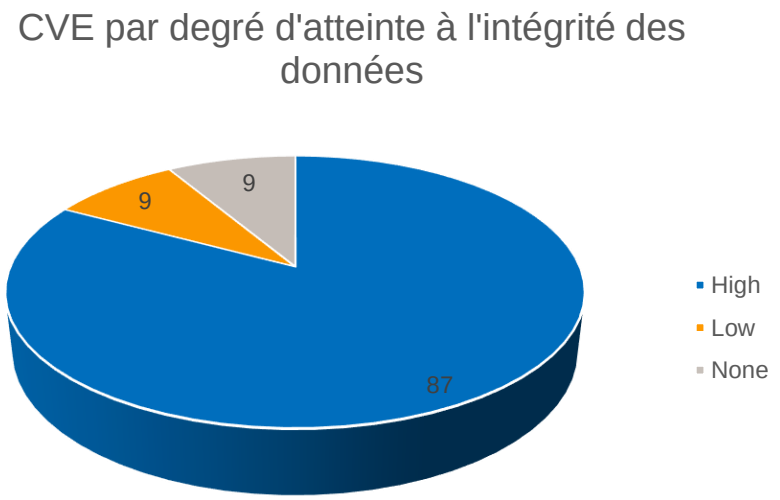
CVE par interaction utilisateur

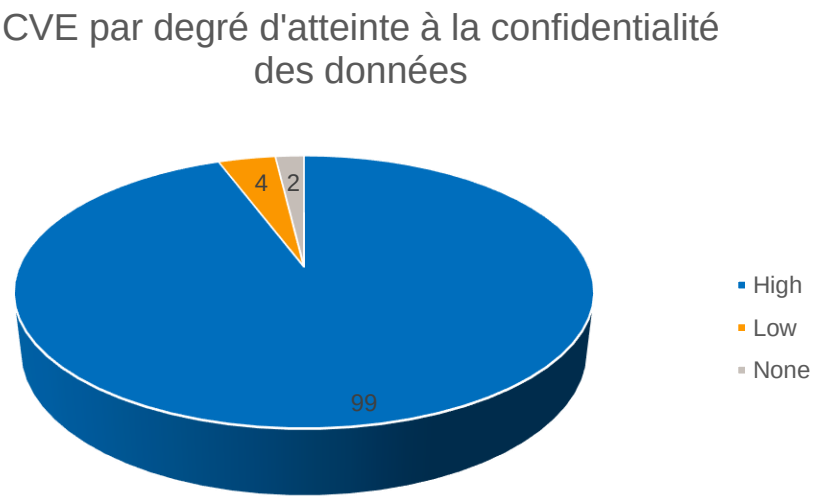


CVE par type de privilèges requis



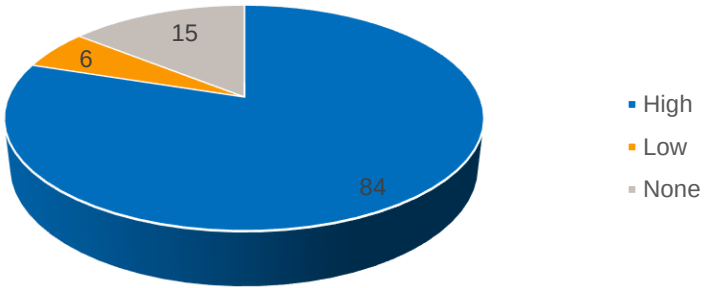
Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données



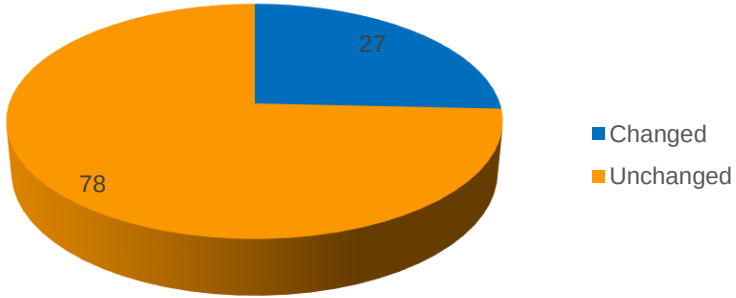


Nombre de CVE selon l'impact sur la disponibilité des données et la portée

CVE par degré d'atteinte à la disponibilité des données



CVE par 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.