CERT Santé

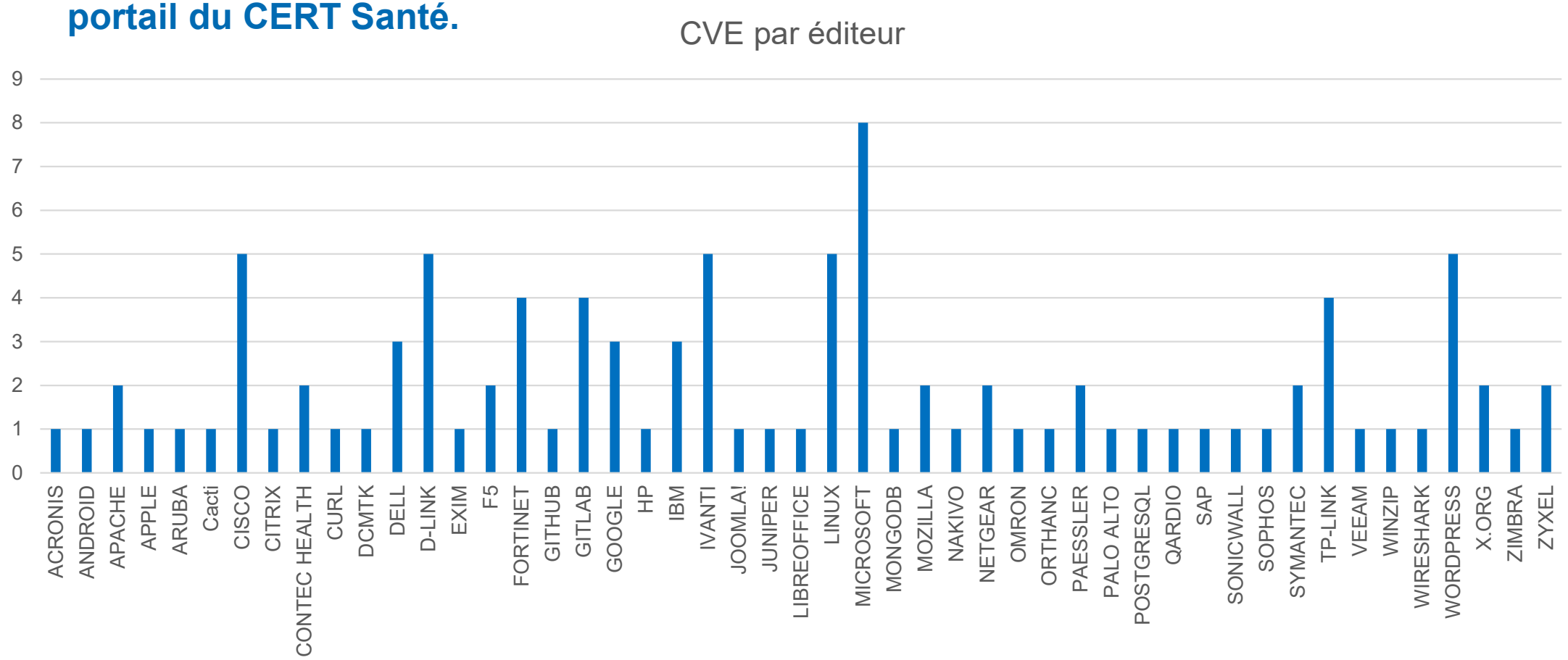
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

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

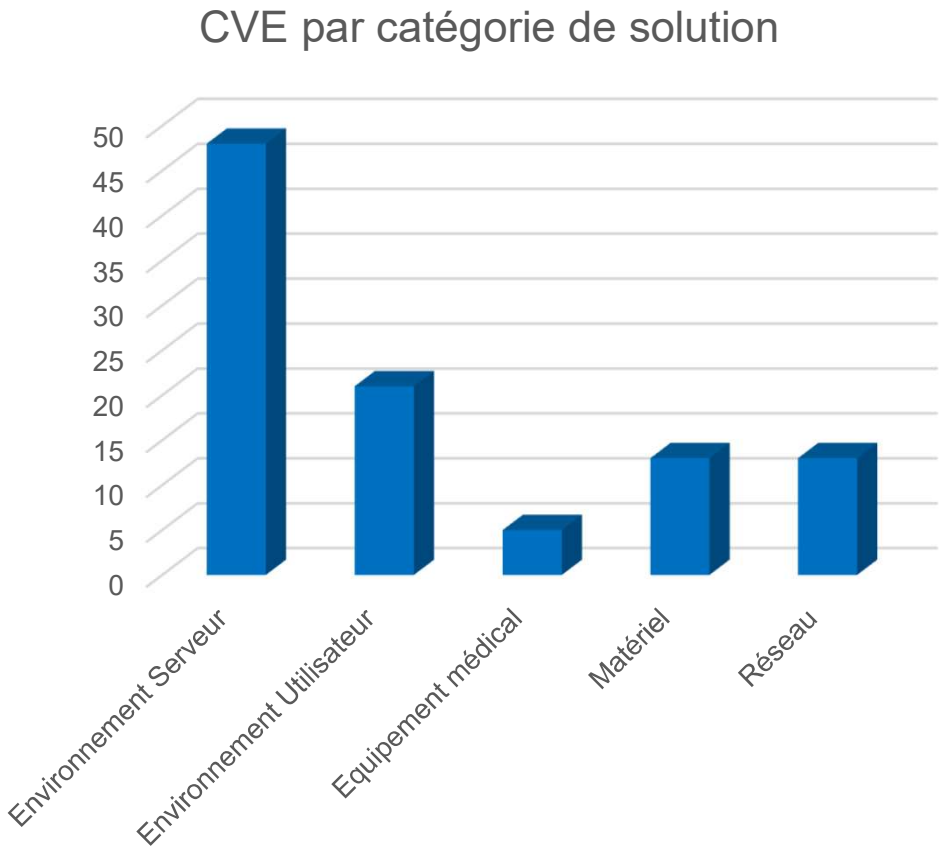
Mars 2025

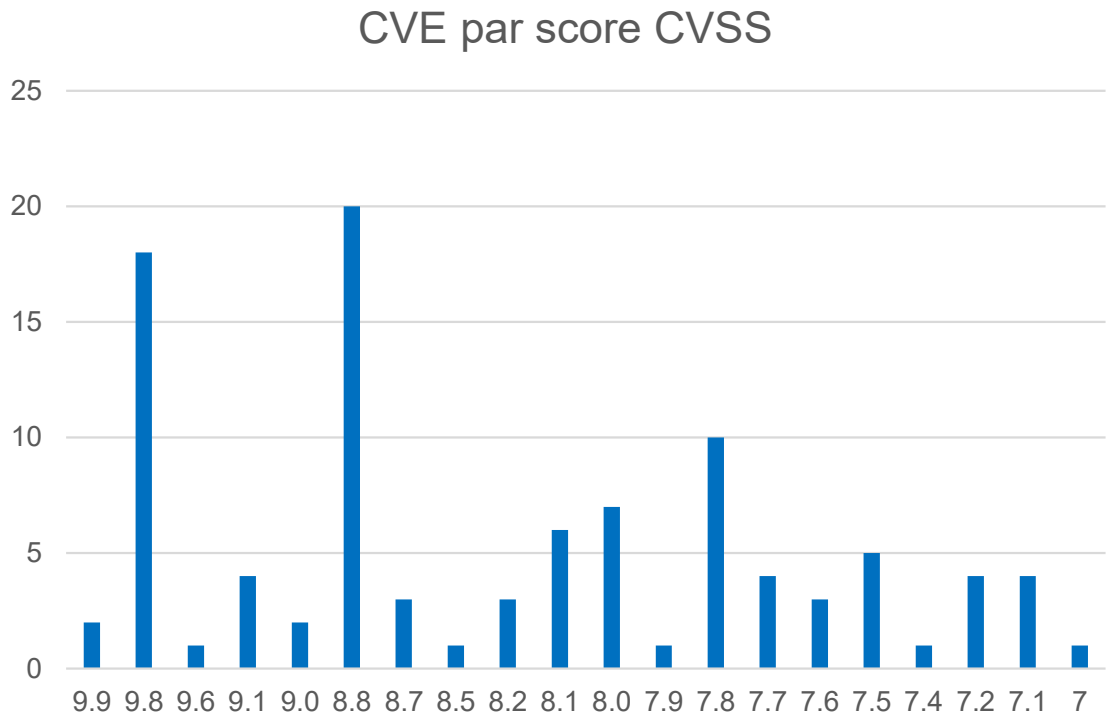
Nombre de CVE par éditeur

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



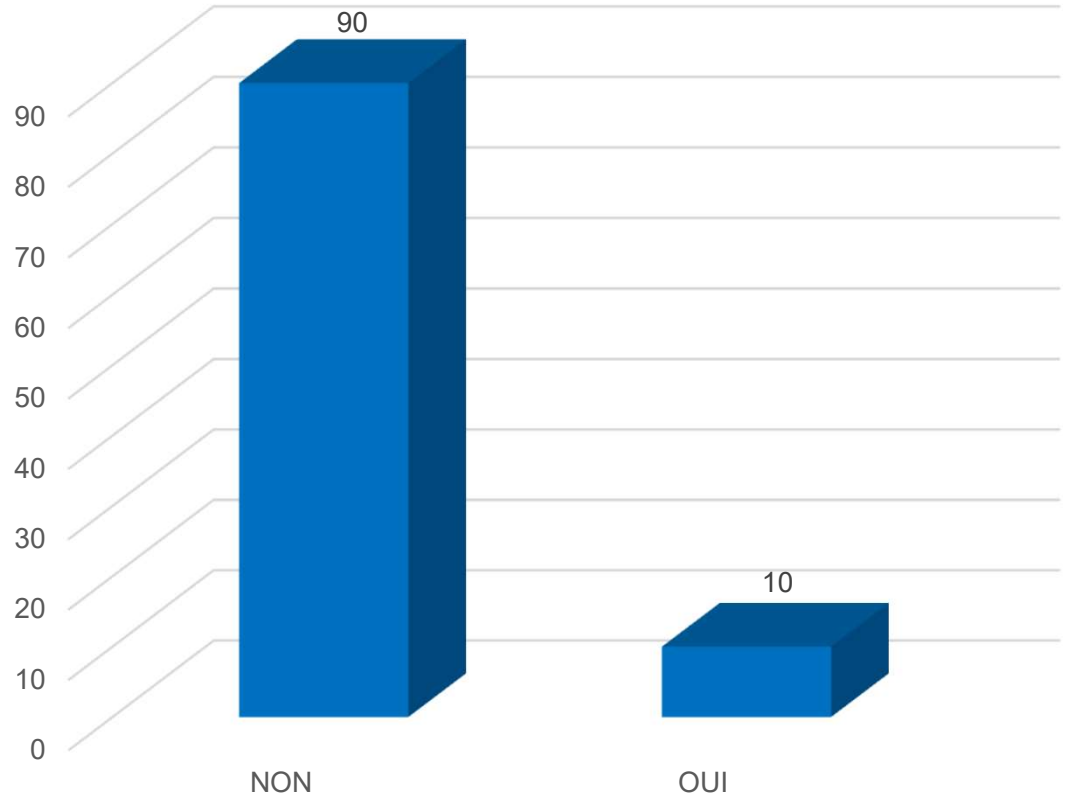
Nombre de CVE par catégorie de produit et score CVSS



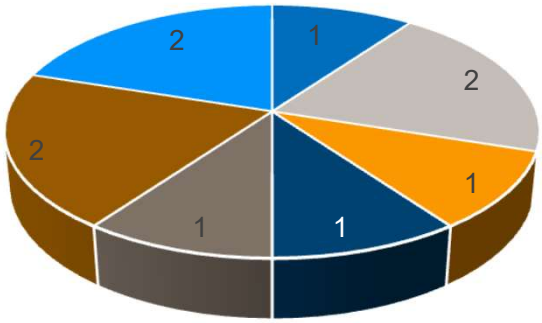


Vulnérabilités exploitées

Failles exploitées

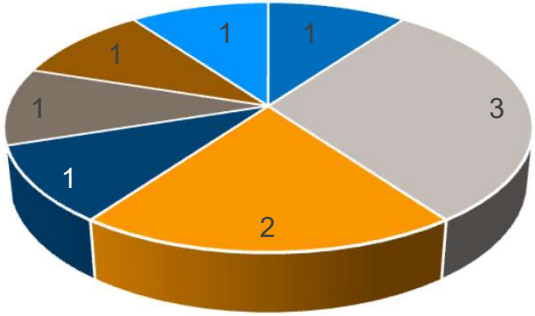


Failles exploitées par type de solution



- Cadre d'application (framework)
- Pare-feu
- Routeur
- Serveur de stockage
- SGBD
- Solution de gestion réseau
- Système d'exploitation

Failles exploitées par éditeur



- ANDROID
- MICROSOFT
- PAESSLER
- PALO ALTO
- POSTGRESQL
- SOPHOS
- ZYXEL

Les vulnérabilités critiques à surveiller

Palo Alto
([CVE-2025-0108](#))

Atteinte à la confidentialité des données

Exploitée

Un défaut de contrôle d'authentification dans la console de gestion web des pare-feux Palo Alto permet à un attaquant ayant un accès réseau à cette interface, d'exécuter des scripts *PHP*, portant atteinte à la confidentialité et l'intégrité des données.

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

Microsoft
([CVE-2025-21391](#))

Elévation de privilèges

Exploitée

Un défaut de gestion des liens dans *Windows Storage* de Microsoft permet à un attaquant authentifié d'élever ses privilèges et de supprimer des fichiers, pouvant affecter la disponibilité du service.

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

PostgreSQL
([CVE-2025-1094](#))

Exécution de code arbitraire

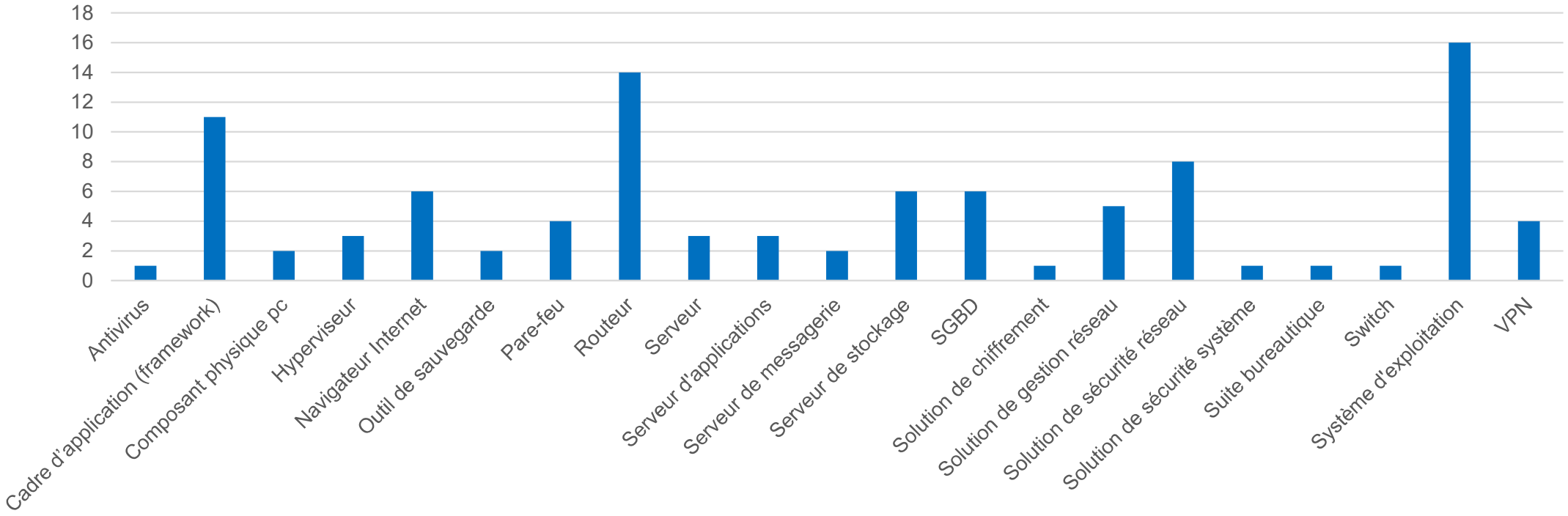
Exploitée

Un défaut de contrôle des requêtes dans PostgreSQL permet à un attaquant, en menant une attaque de type injection SQL, d'exécuter du code arbitraire.

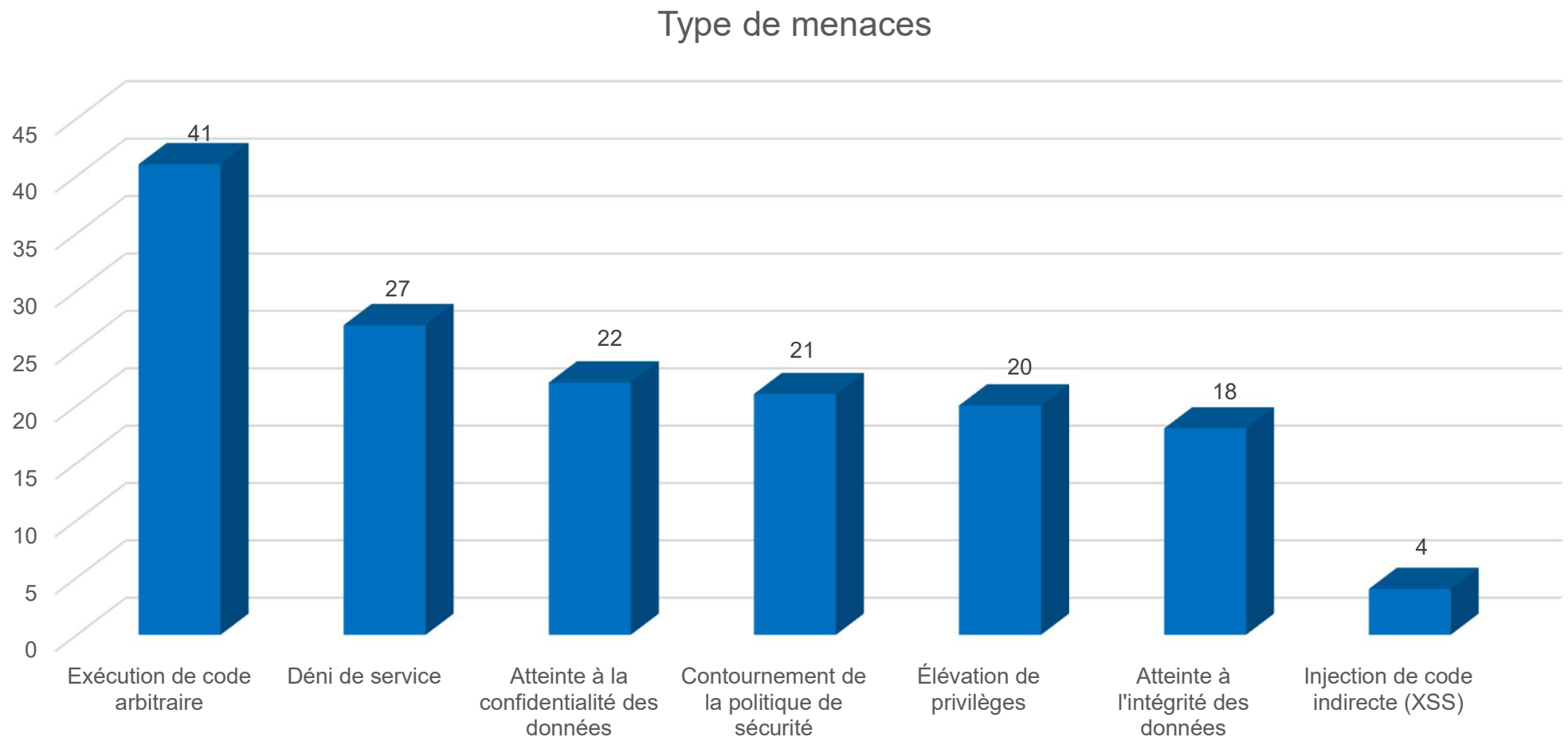
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

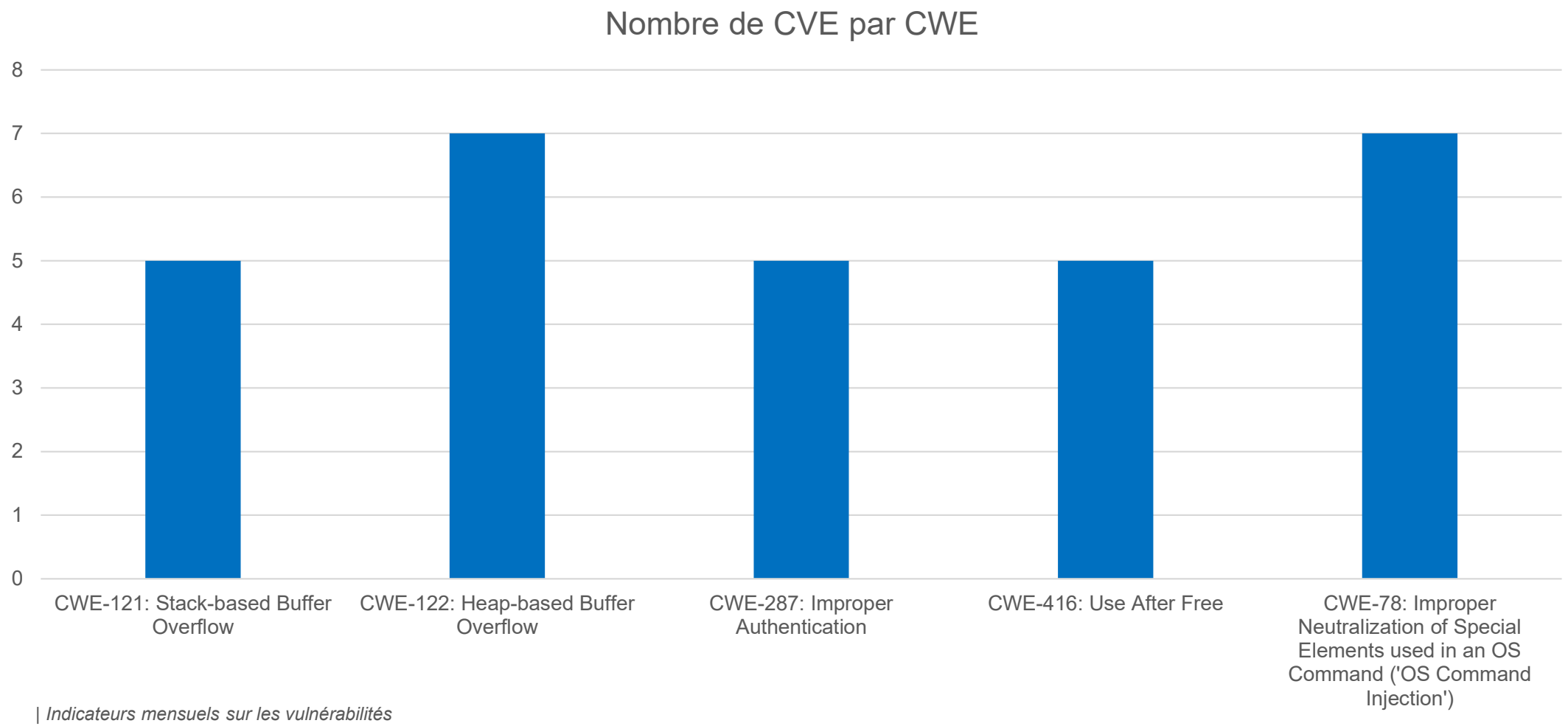
Les systèmes d'exploitation, les cadres d'application, les routeurs et les navigateurs internet sont les principaux types d'équipements affectés par les vulnérabilités publiées.



Types de menaces

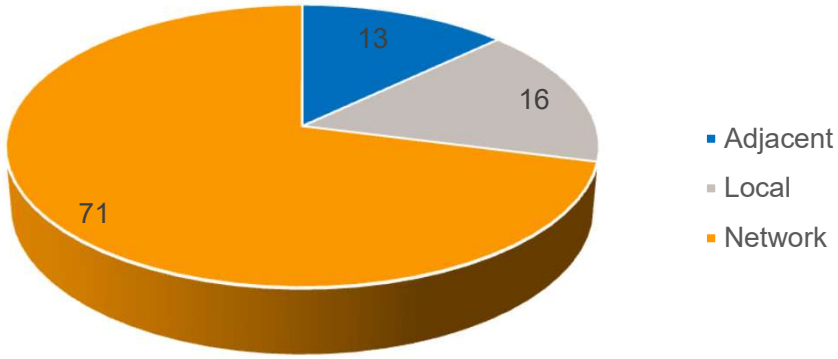


TOP 5 des failles selon le référentiel CWE

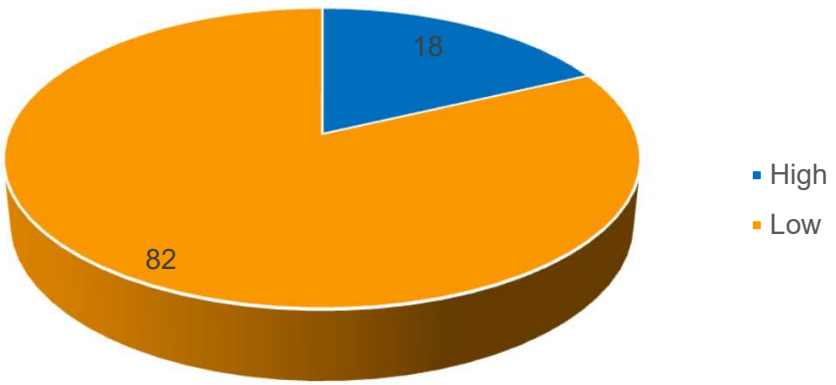


Nombre de CVE selon le vecteur d'attaque et la complexité de l'attaque

CVE par type de vecteur d'attaque

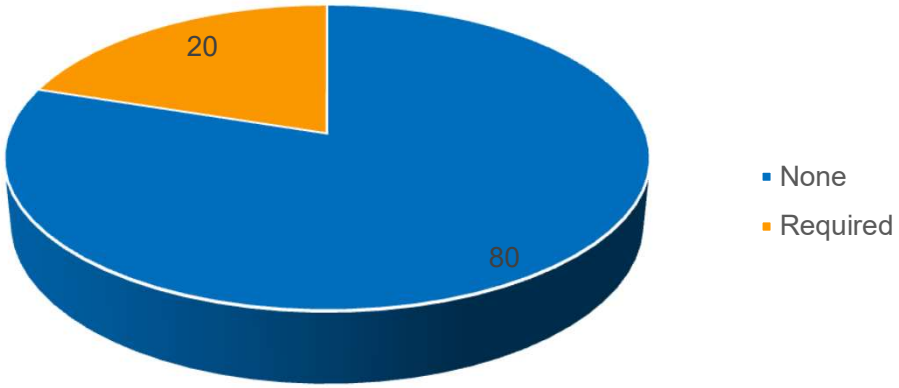


CVE par complexité d'attaque

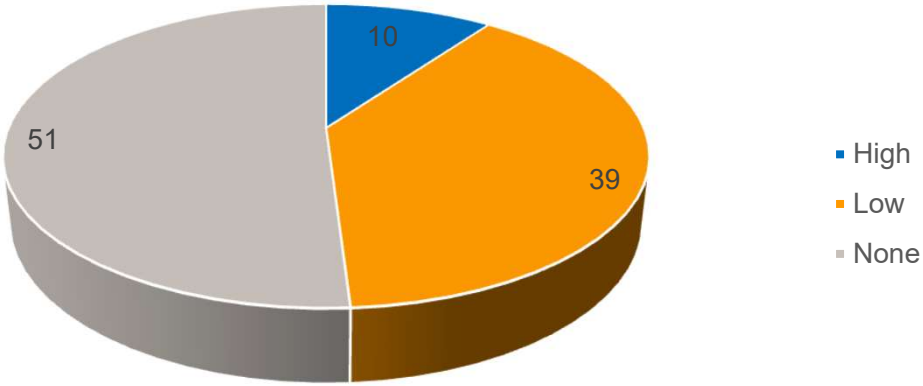


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

CVE par interaction utilisateur

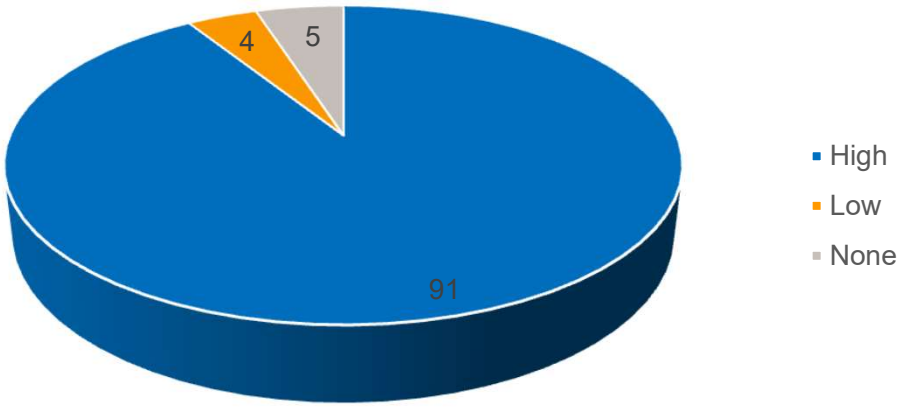


CVE par type de privilèges requis

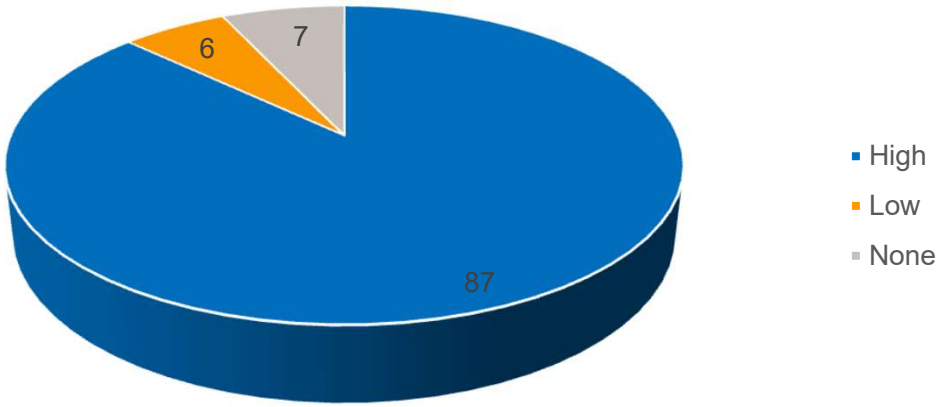


Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données

CVE par degré d'atteinte à l'intégrité des données

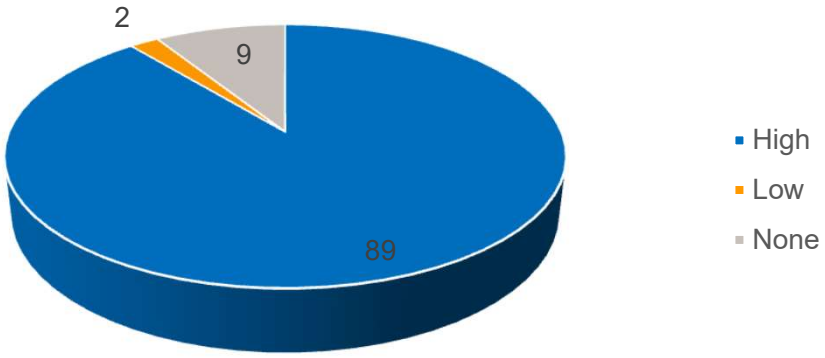


CVE par degré d'atteinte à la confidentialité des données

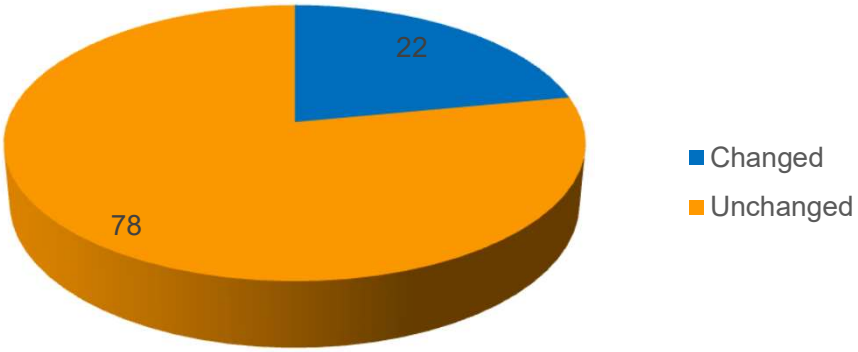


Nombre de CVE selon l'impact sur la disponibilité des données et la portée

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.