



**AGENCE
DU NUMÉRIQUE
EN SANTÉ**

La transformation commence ici 



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

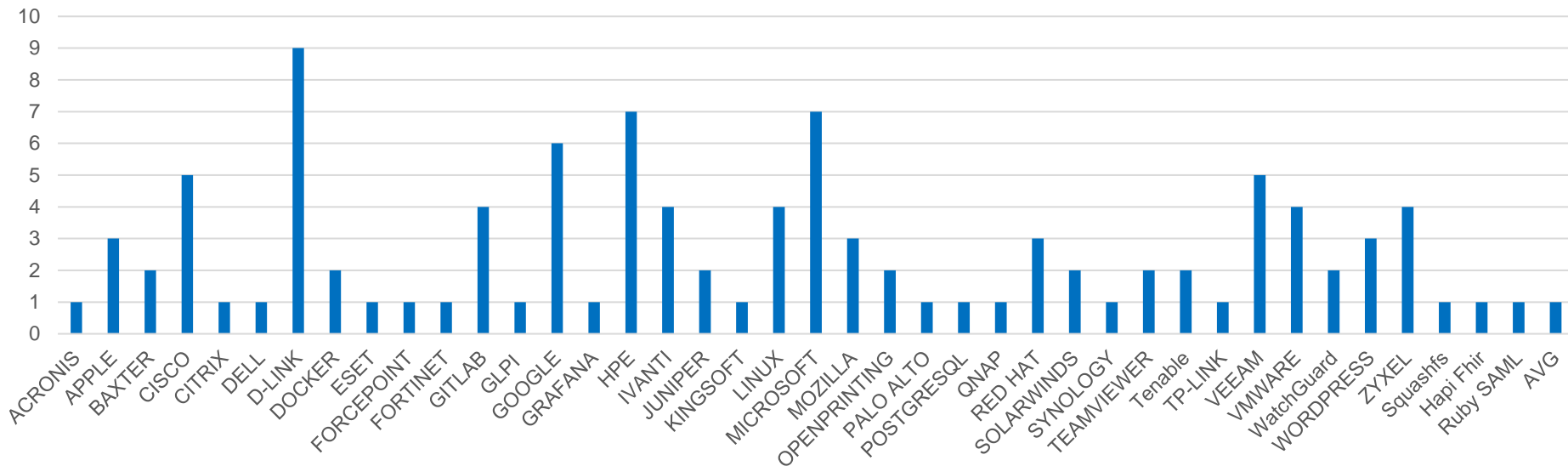
CERT Santé

Octobre 2024

Nombre de CVE par éditeur

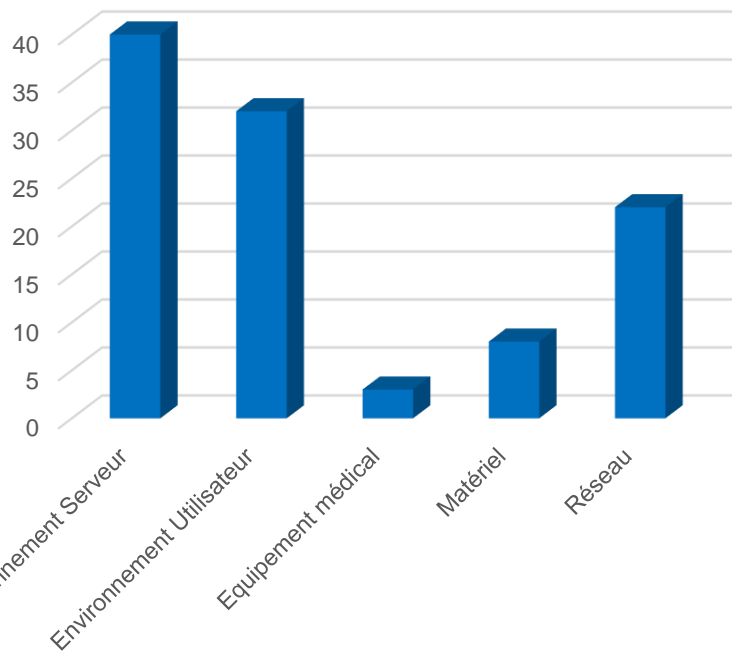
105 vulnérabilités ont été analysées et publiées (parmi lesquelles 6 alertes) sur le portail du CERT Santé.

CVE par éditeur

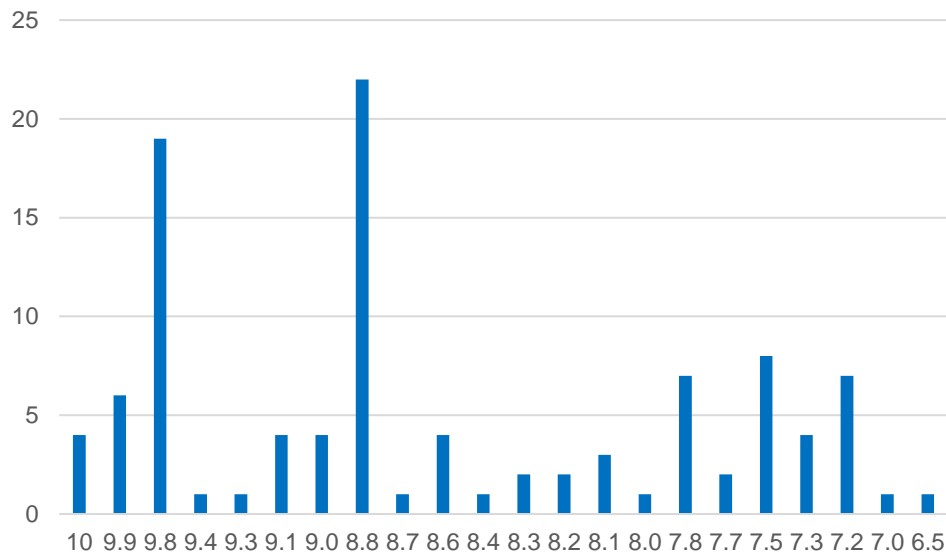


Nombre de CVE par catégorie de produit et score CVSS

CVE par catégorie de solution

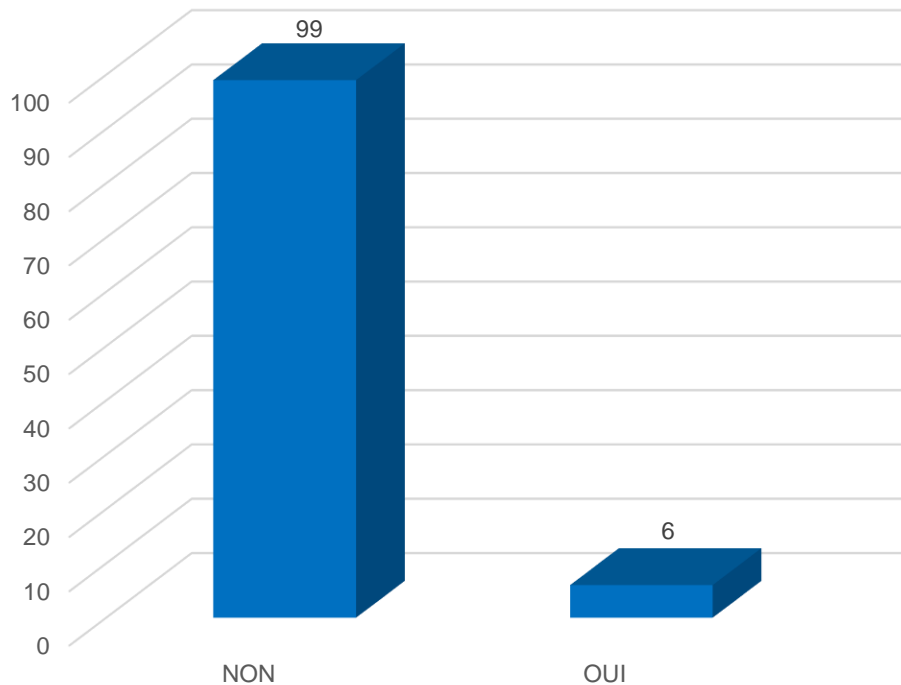


CVE par score CVSS

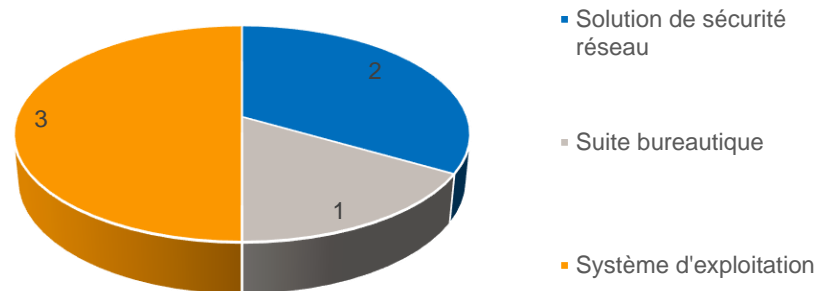


Vulnérabilités exploitées

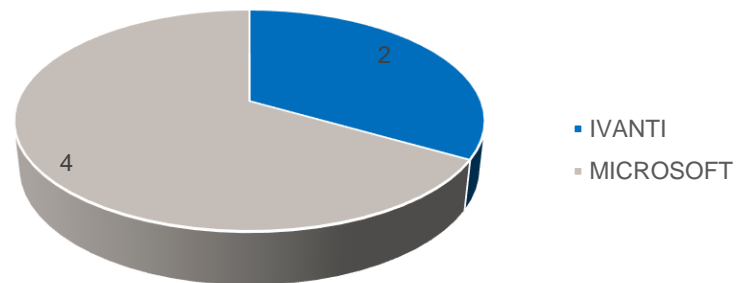
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

9.8

Microsoft

([CVE-2024-43491](#))

Exécution de code
arbitraire

Exploitée

Un défaut dans le Servicing Stack affectant certains composants Microsoft Windows 10 permet à un attaquant d'exécuter du code arbitraire.

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

9.4

Ivanti

([CVE-2024-8963](#))

Contournement de la
politique de sécurité

Exploitée

Une vulnérabilité de type « traversée de répertoire » dans Ivanti CSA permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'accéder à des fonctionnalités restreintes.

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

9

Cups

([CVE-2024-47177](#))

Exécution de code
arbitraire

PoC

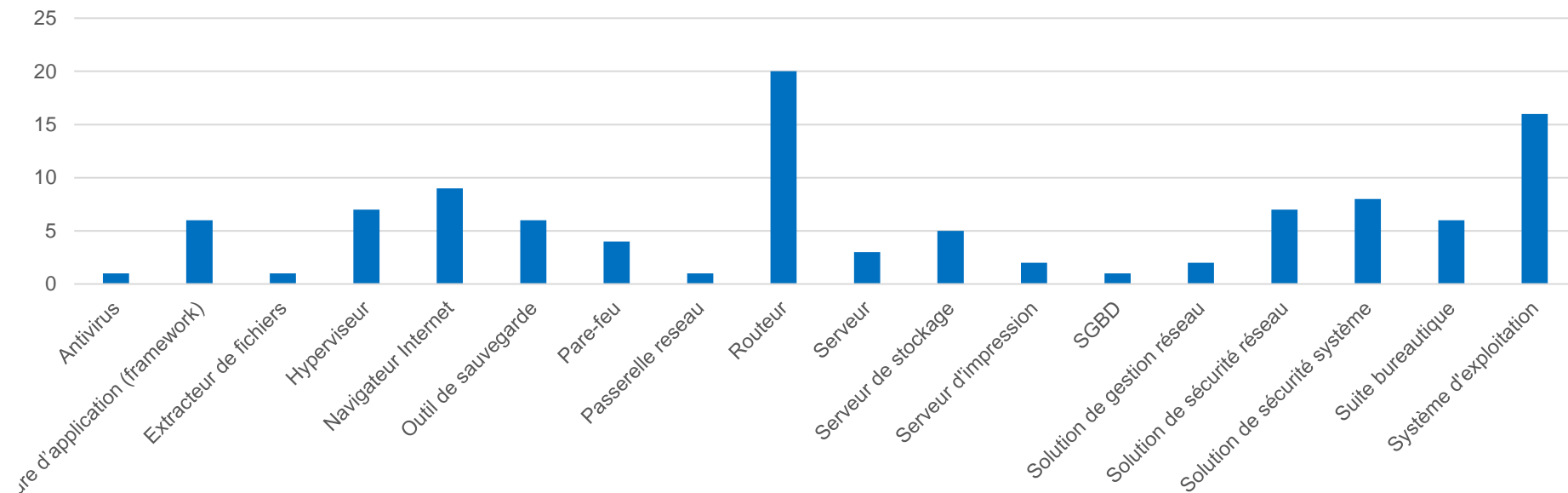
Une vulnérabilité de type injection de commande dans le paquet cups-filters permet à un attaquant non authentifié, en envoyant un fichier PPD (Postscript Printer Description) spécifiquement forgé, d'exécuter des commandes arbitraires.

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

Types de solutions vulnérables

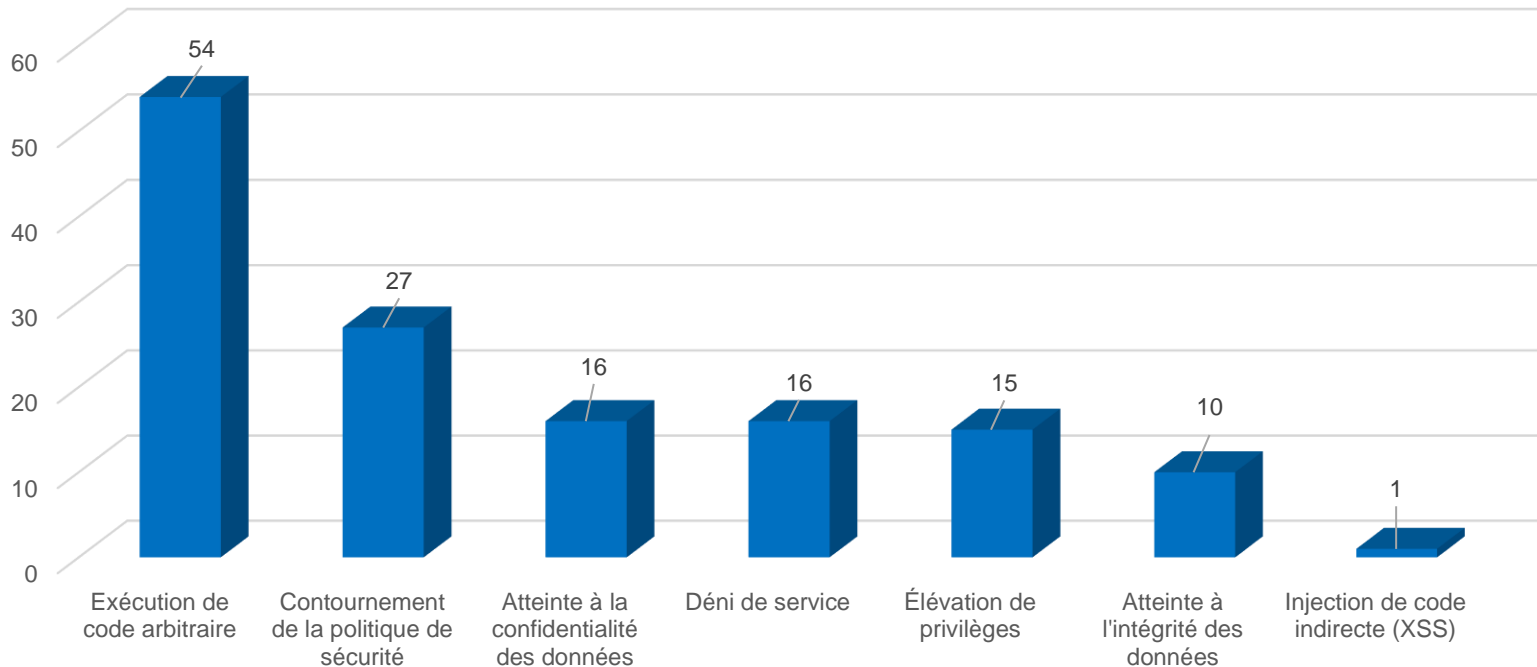
Les routeurs, les systèmes d'exploitation, les solutions de sécurité systèmes et les navigateurs internet sont les principaux types d'équipements affectés par les vulnérabilités publiées.

CVE par type de solution



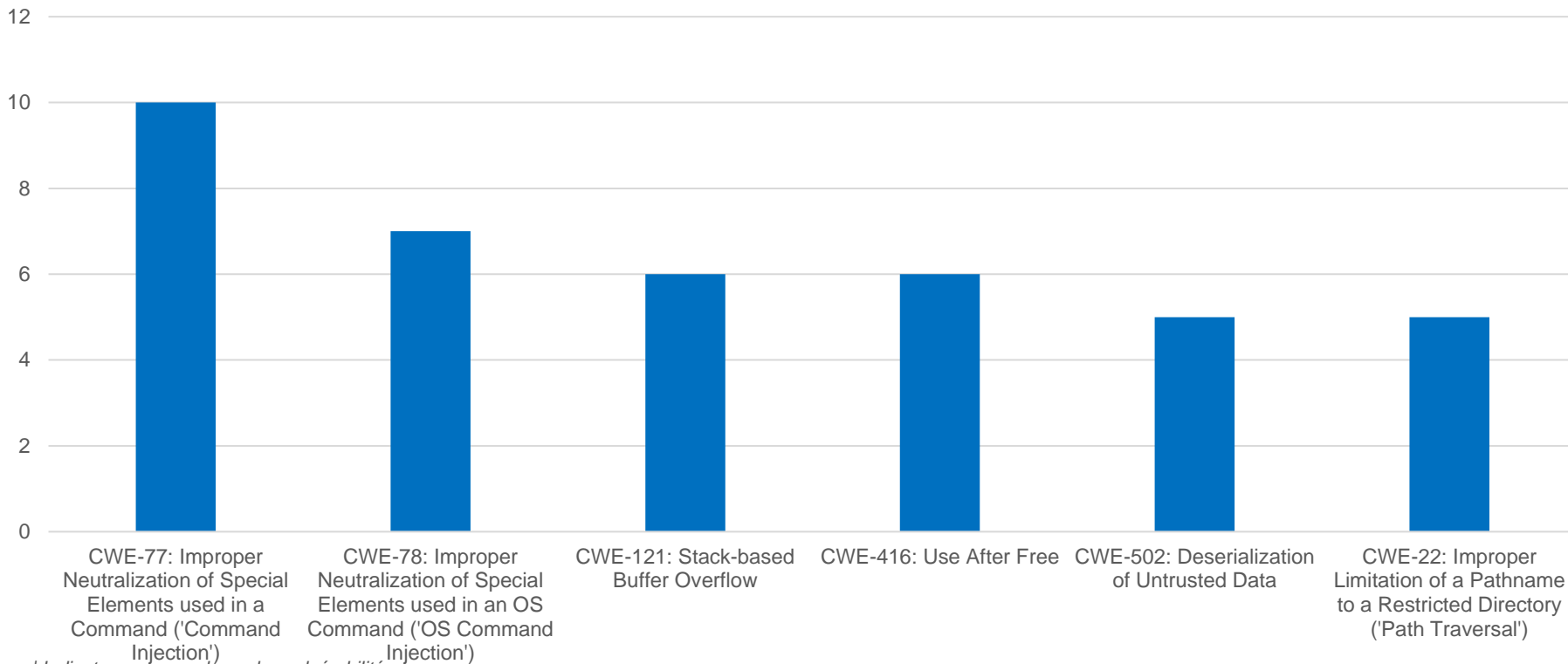
Types de menaces

Type de menaces



TOP 6 des failles selon le référentiel CWE

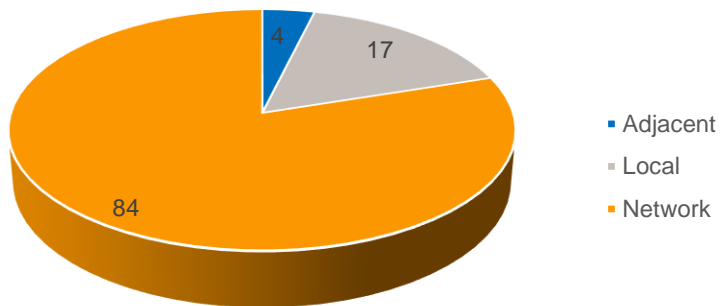
Nombre de CVE par CWE



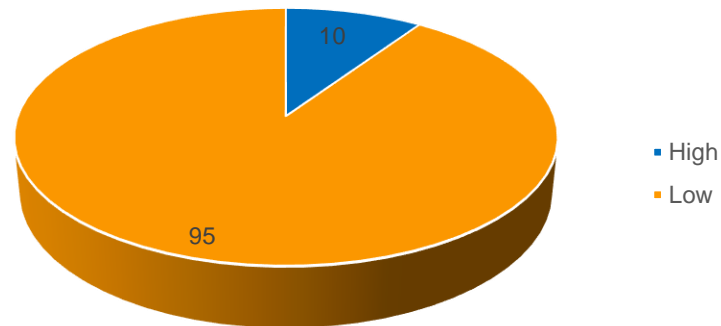
| Indicateurs mensuels sur les vulnérabilités

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

CVE par type de vecteur d'attaque

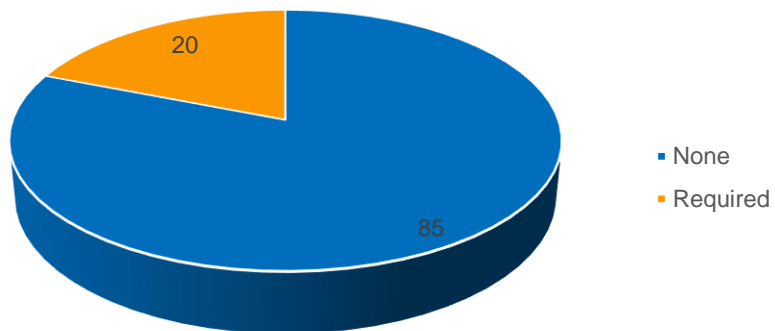


CVE par complexité d'attaque

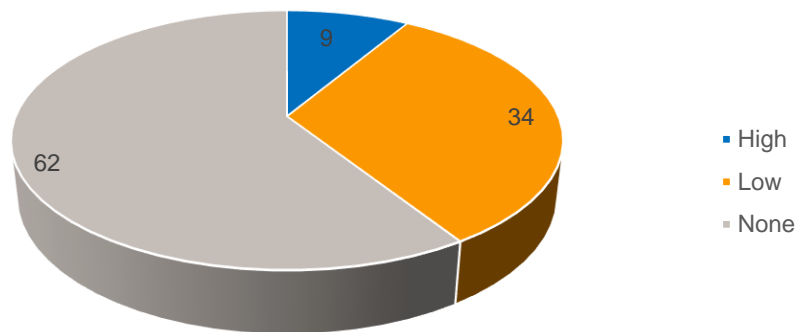


Nombre de CVE selon les conditions de l'exploitation de la vulnérabilité

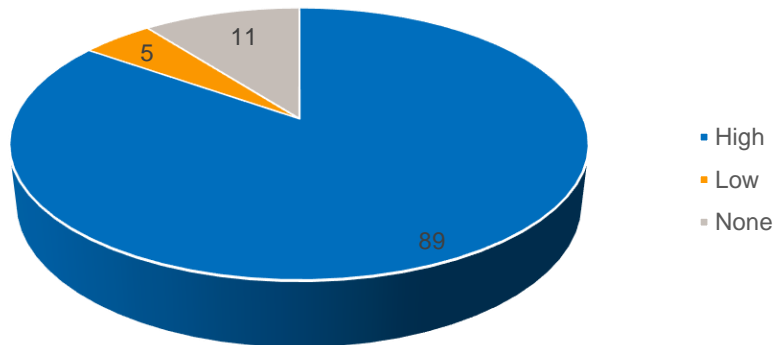
CVE par interaction utilisateur



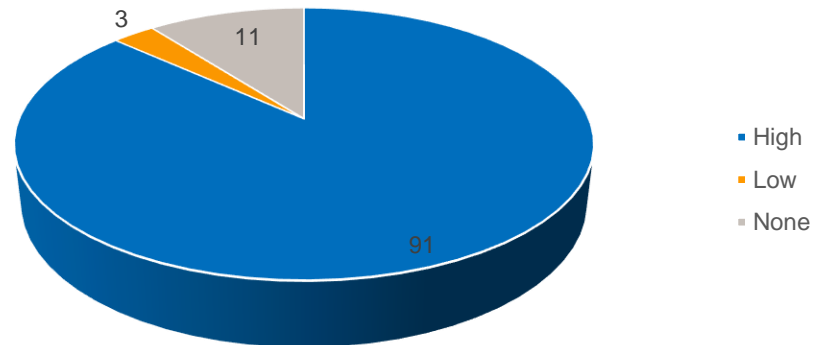
CVE par type de privilèges requis



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

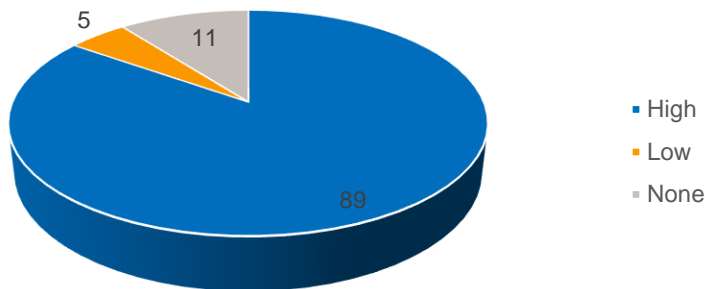


CVE par degré d'atteinte à la confidentialité des données

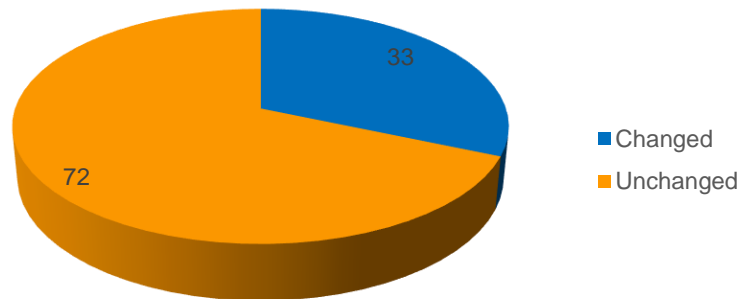


Nombre de CVE selon l'impact sur la disponibilité des données et la portée

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.