AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

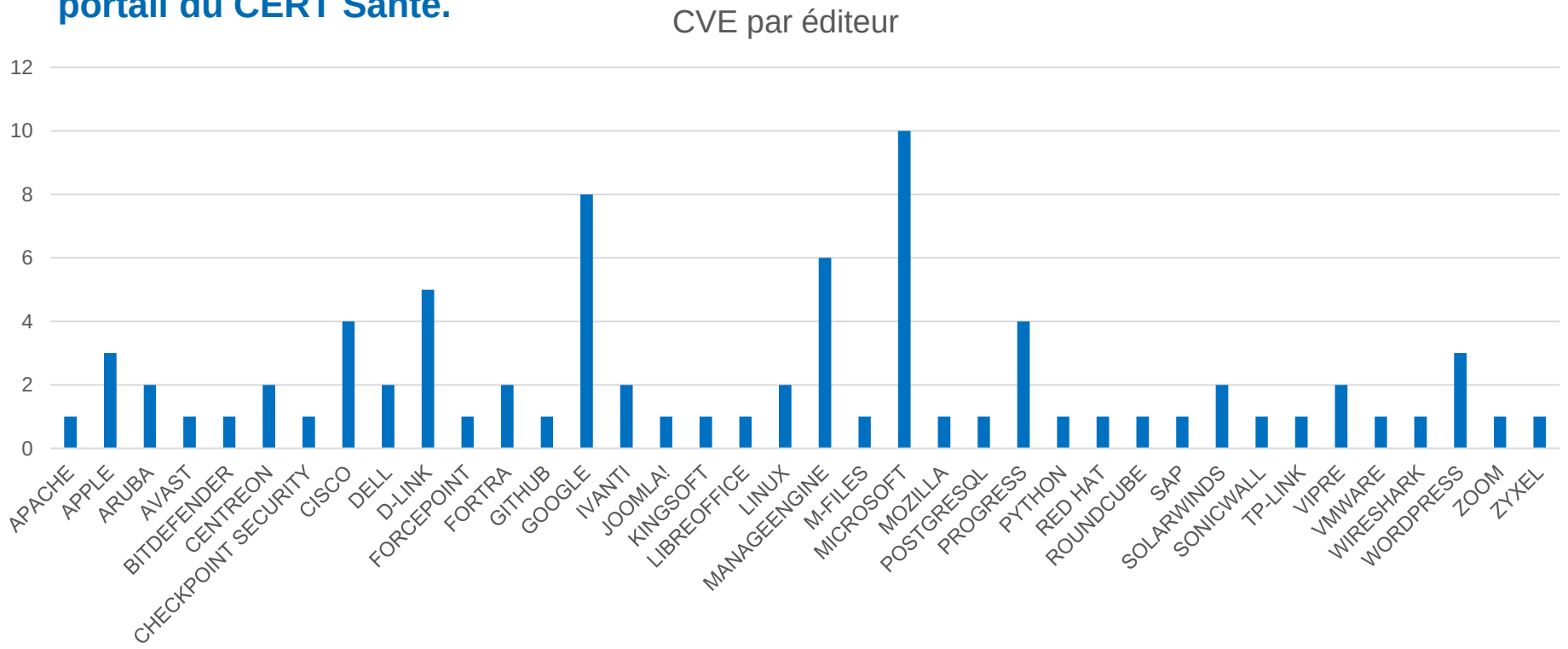
# Indicateurs sur la publication des CVE pour le mois d'août 2024

## CERT Santé

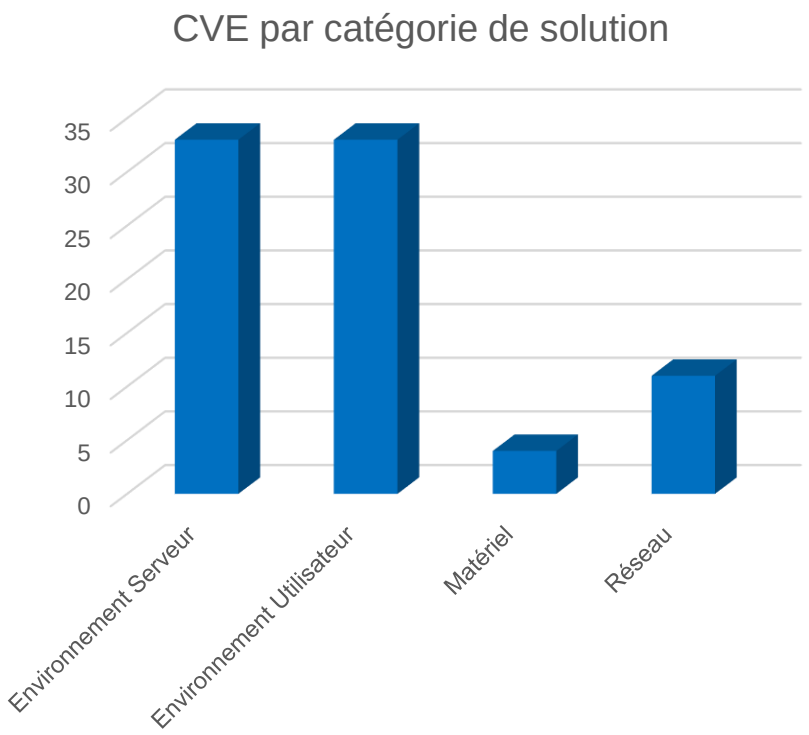
**Septembre 2024**

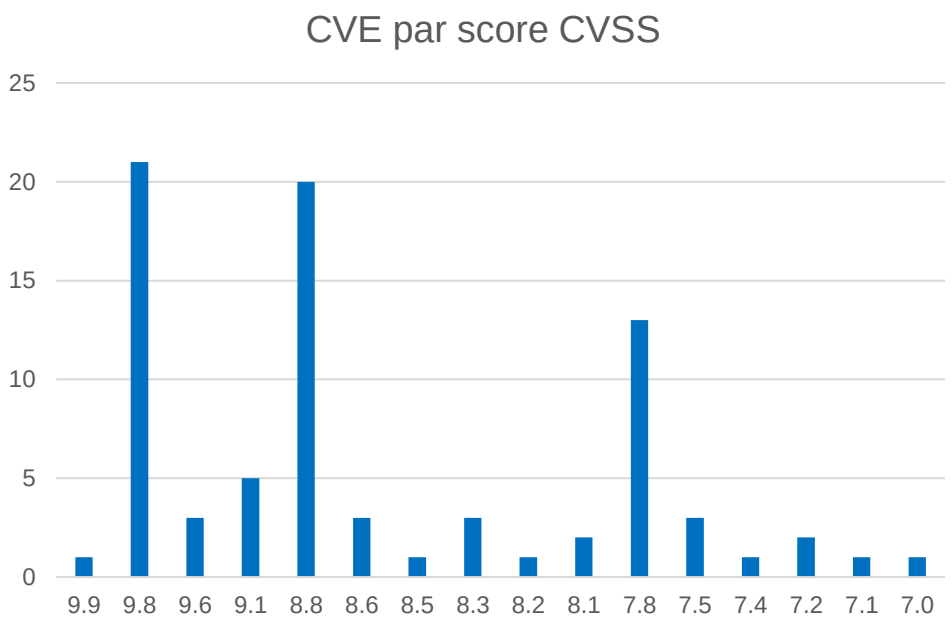
# Nombre de CVE par éditeur

## 81 vulnérabilités ont été analysées et publiées (parmi lesquelles 13 alertes) sur le portail du CERT Santé.



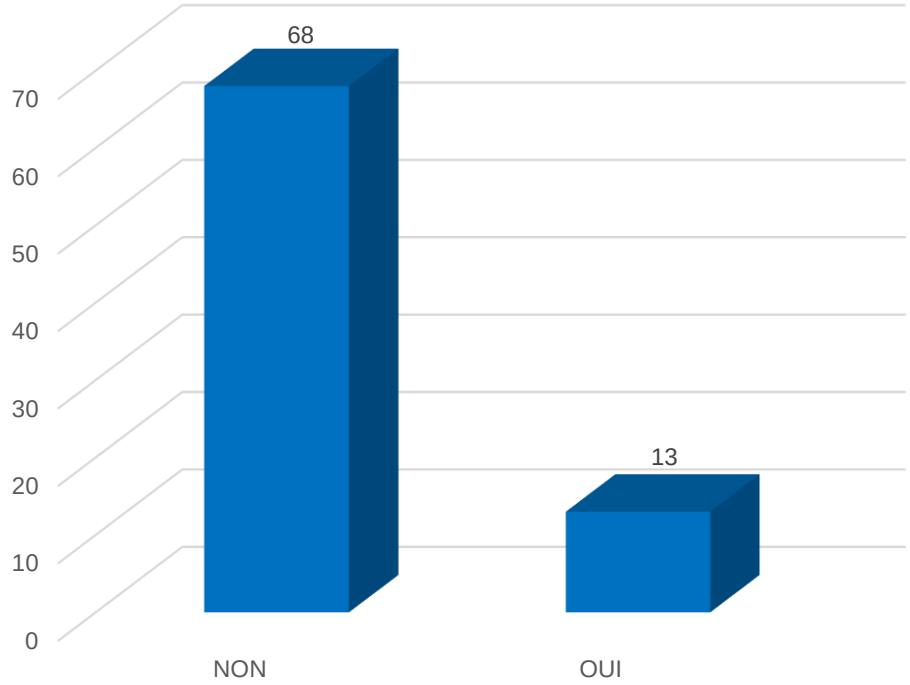
# Nombre de CVE par catégorie de produit et score CVSS



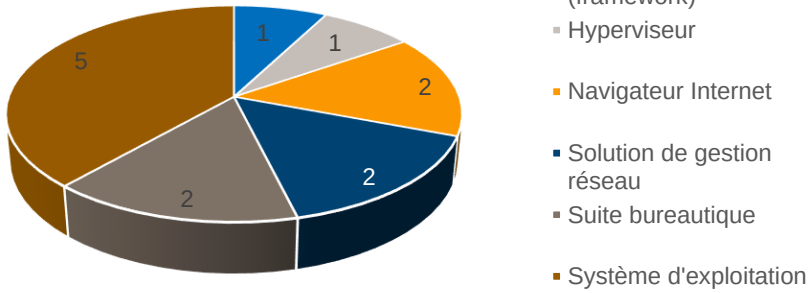



# Vulnérabilités exploitées

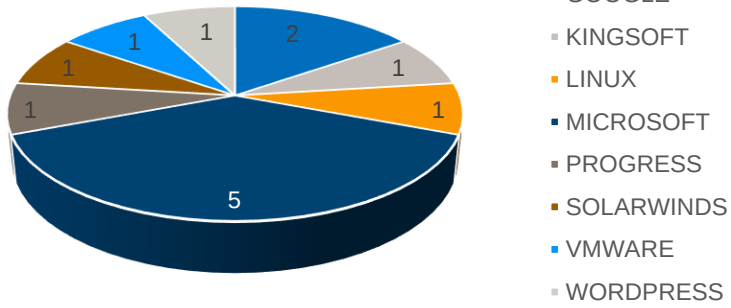
## Failles exploitées




## Failles exploitées par type de solution




## Failles exploitées par éditeur



# Les vulnérabilités critiques à surveiller


## SolarWinds

Exécution de code arbitraire

Exploitée

**(CVE-2024-29886)**

Un défaut de désérialisation Java dans SolarWinds Web Help Desk permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire

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


## Progress WhatsUp

Exécution de code arbitraire

Exploitée

**(CVE-2024-4885)**

Un défaut de contrôle des extensions de fichier dans la fonction *WhatsUp.ExportUtilities.Export.GetFileWithoutZip* de Progress WhatsUp Gold permet à un attaquant non authentifié, en envoyant des requêtes HTTP spécifiquement forgées, de téléverser un script malveillant et de l'exécuter avec les privilèges *iisapppool\nmconsole*.

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


## Microsoft

Exécution de code arbitraire

Exploitée

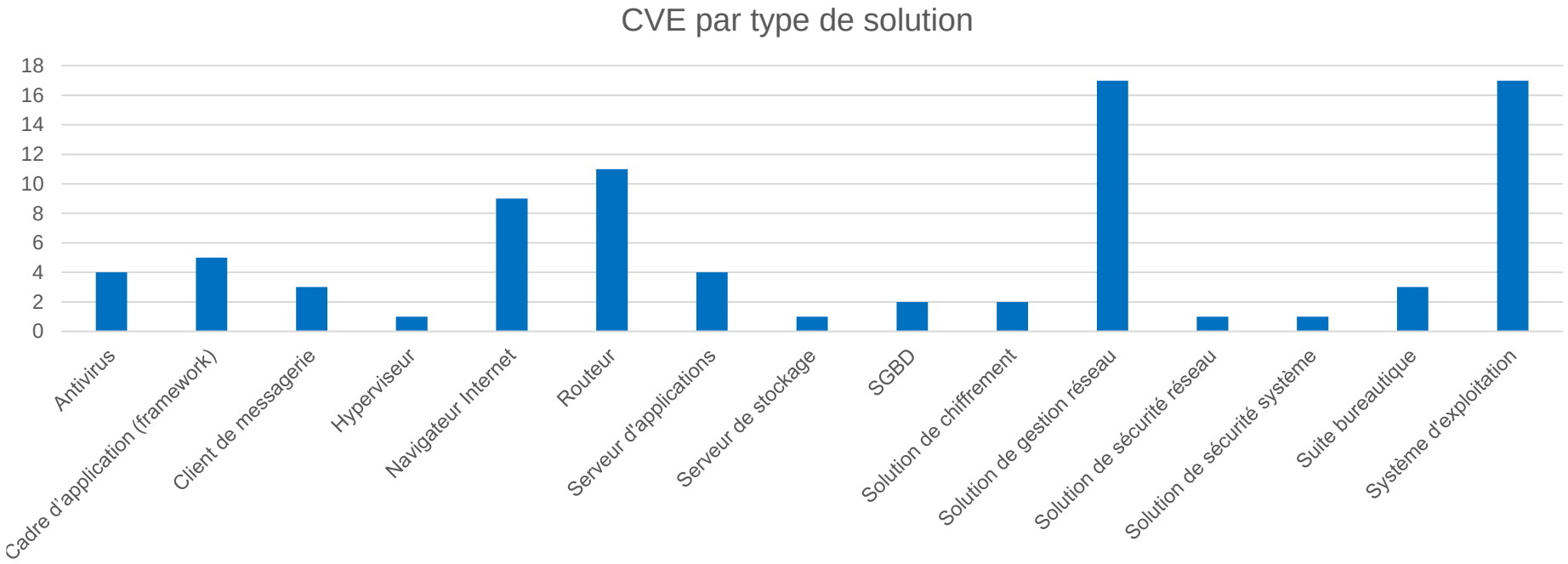
**(CVE-2024-38189)**

Un défaut de contrôle des données envoyées par l'utilisateur dans Microsoft Office et Project permet à un attaquant non authentifié, en persuadant une victime de consulter un fichier spécifiquement forgé, d'exécuter du code arbitraire.

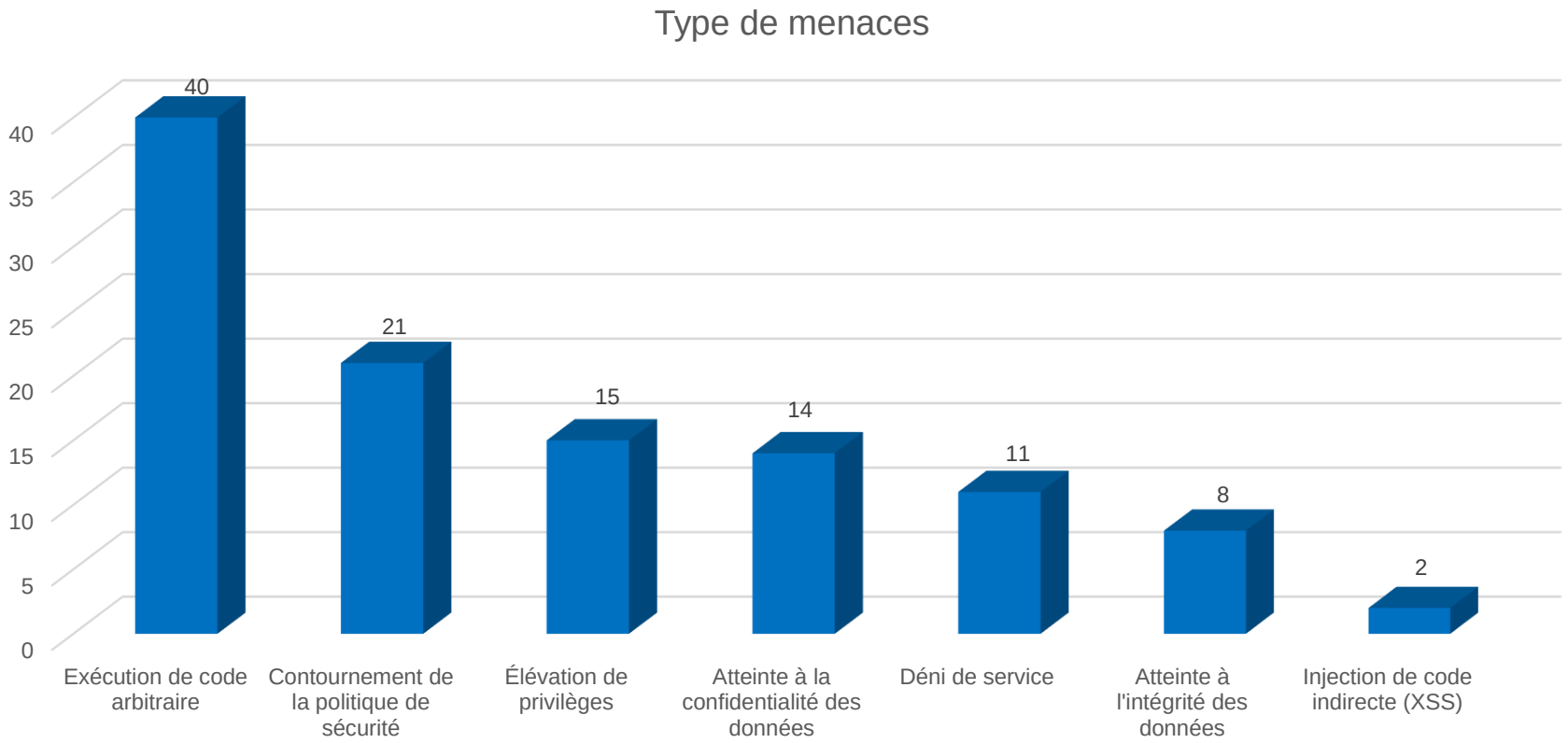
**Recommandations** : Appliquez les correctifs conformément aux instructions de l'éditeur.

# Types de solutions vulnérables

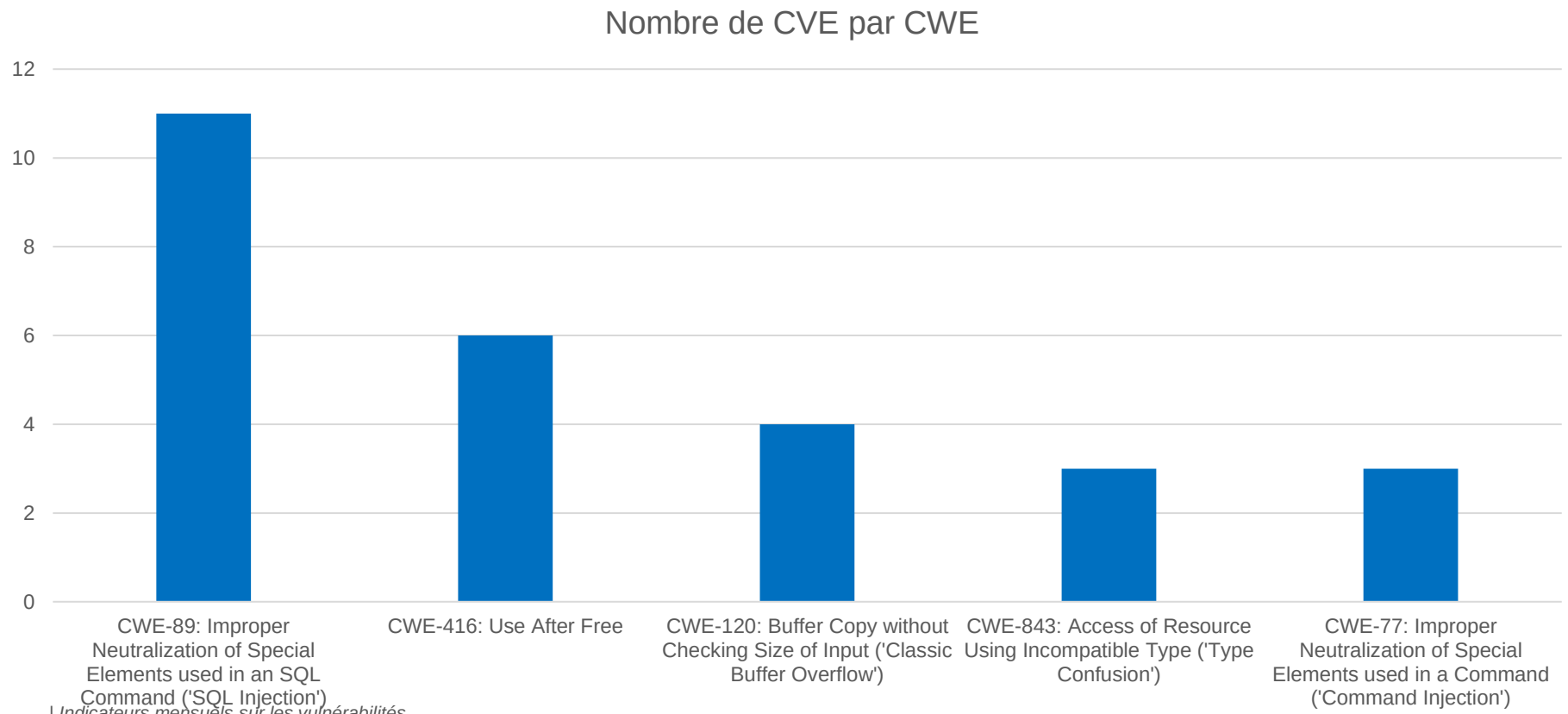
## Les systèmes d'exploitation, les solutions de gestion réseau et les routeurs sont les principaux types d'équipements affectés par les vulnérabilités publiées.



# Types de menaces

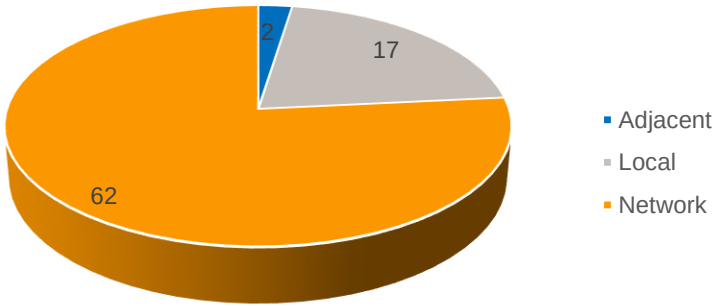


# TOP 5 des failles selon le référentiel CWE

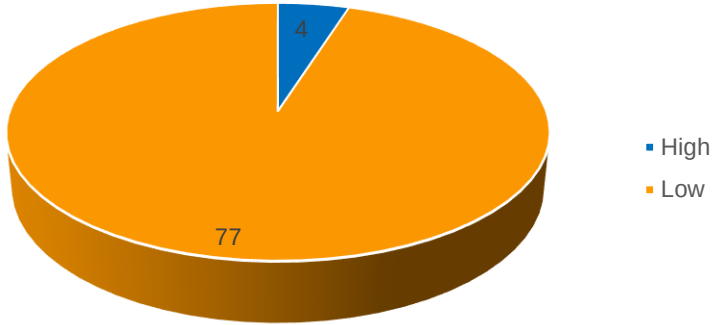


# Nombre de CVE selon le vecteur d’attaque et la complexité de l’attaque

CVE par type de vecteur d'attaque

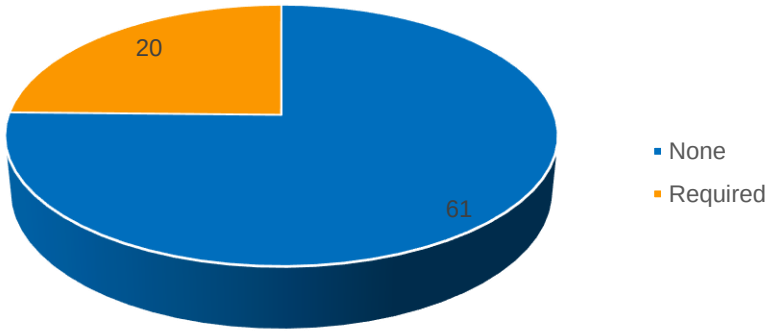



CVE par complexité d'attaque

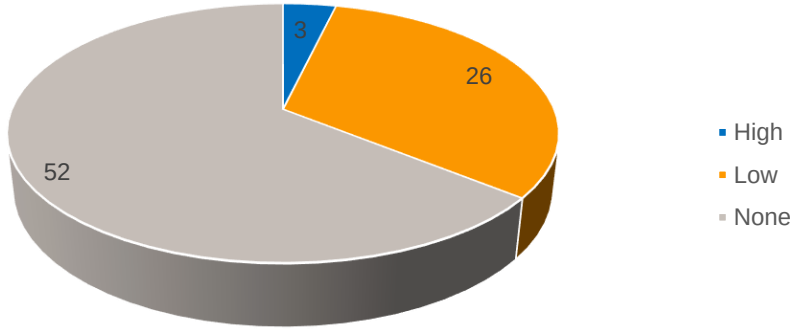


# Nombre de CVE selon les conditions de l’exploitation de la vulnérabilité

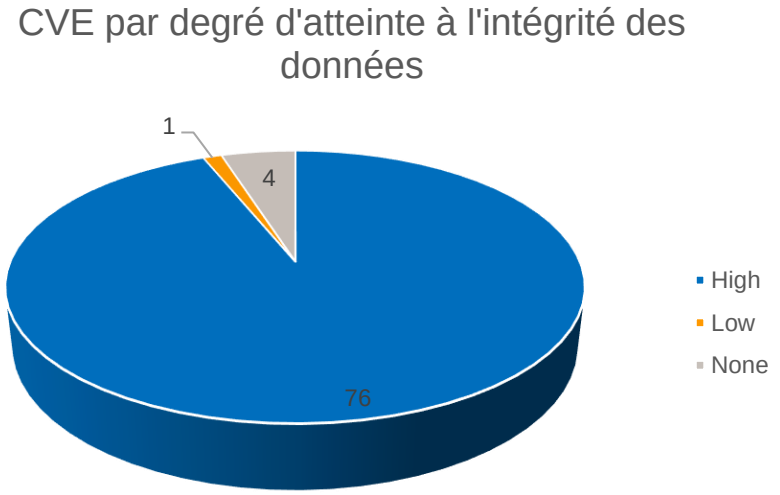
CVE par interaction utilisateur

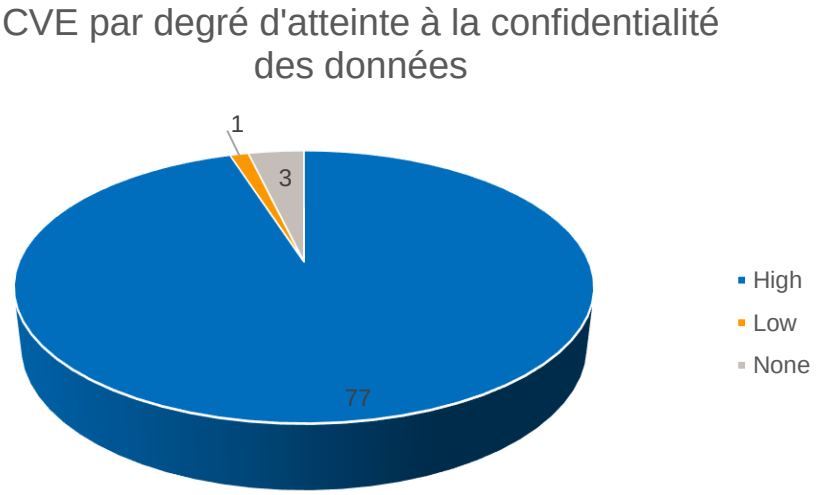



CVE par type de privilèges requis

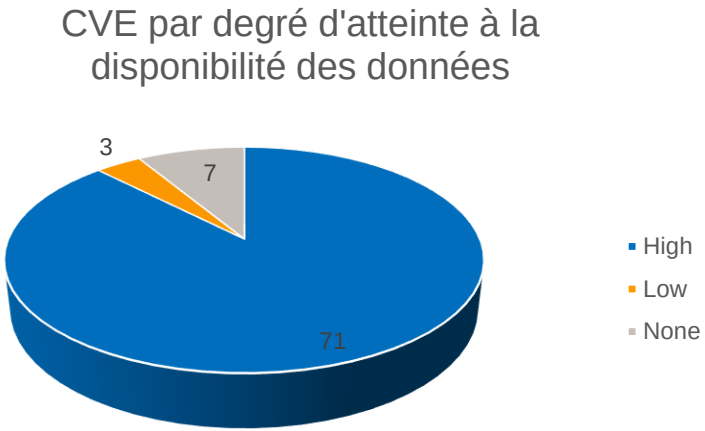


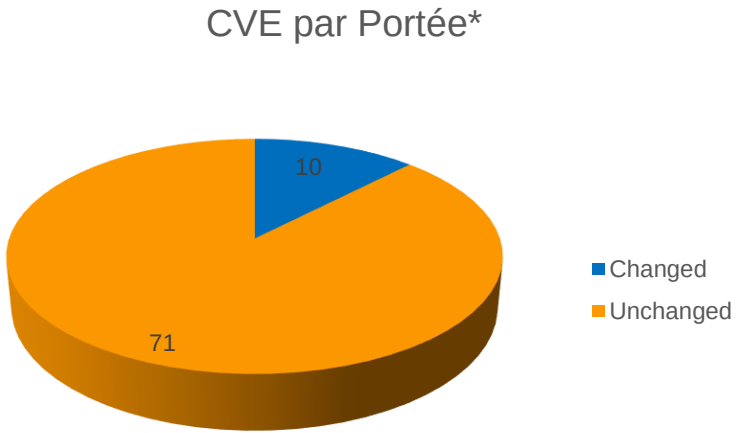
# Nombre de CVE selon l'impact sur l'intégrité et sur la confidentialité des données



# 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.