



**AGENCE  
DU NUMÉRIQUE  
EN SANTÉ**

La transformation commence ici 



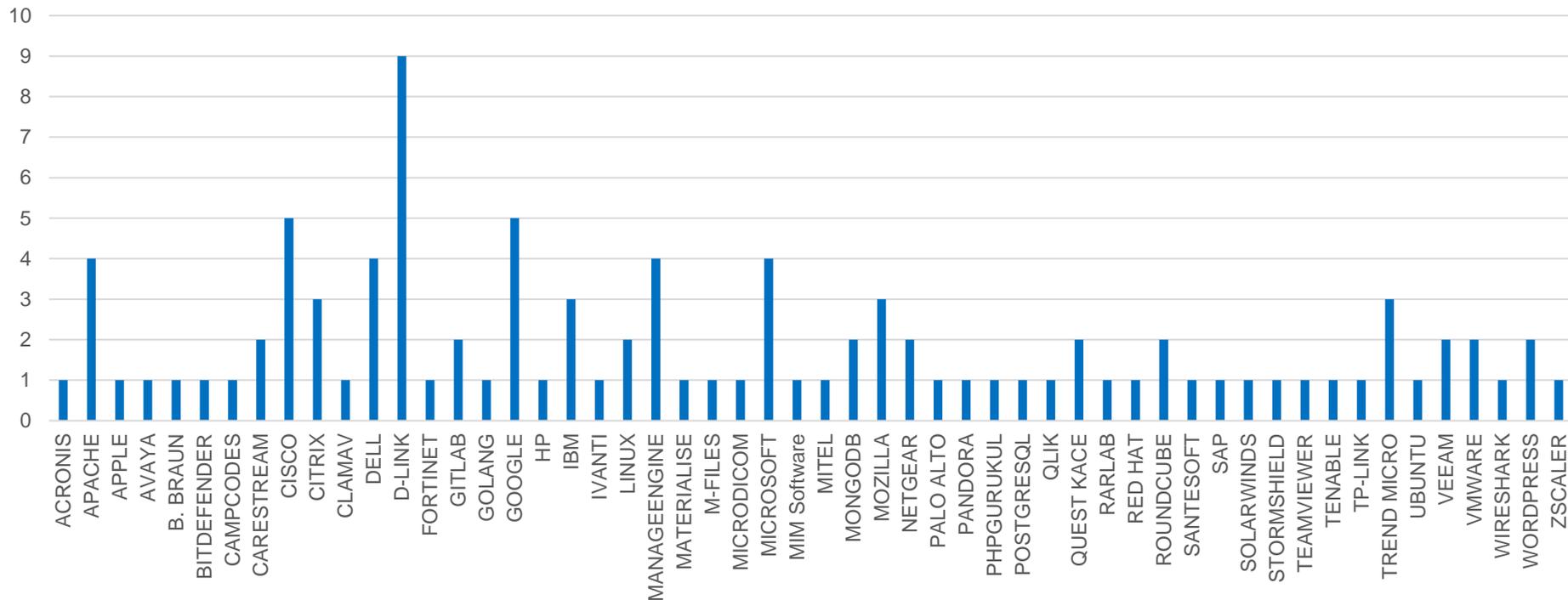
# Indicateurs sur la publication des CVE pour le mois de juin 2025

**Juillet 2025**

# Nombre de CVE par éditeur

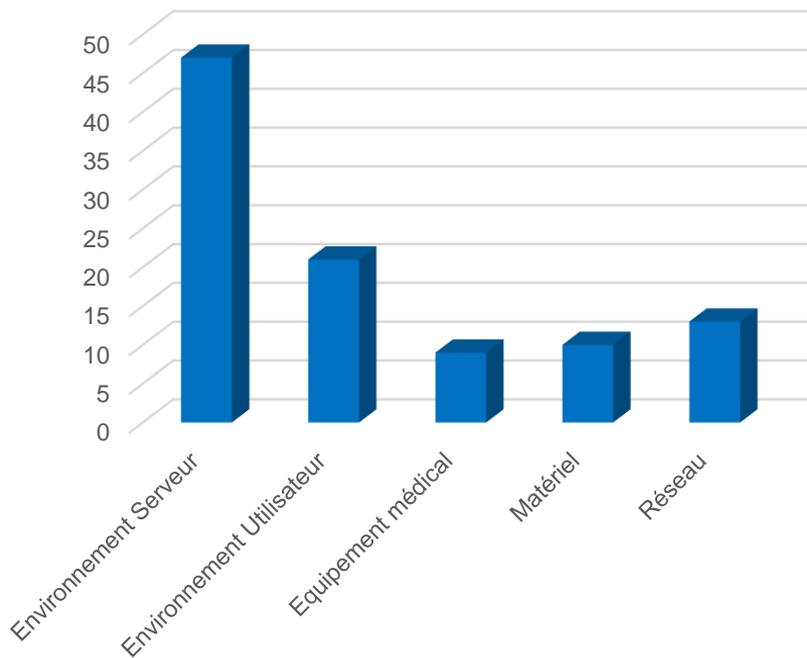
100 vulnérabilités ont été analysées et publiées (parmi lesquelles 6 alertes) sur le portail du CERT Santé.

CVE par éditeur

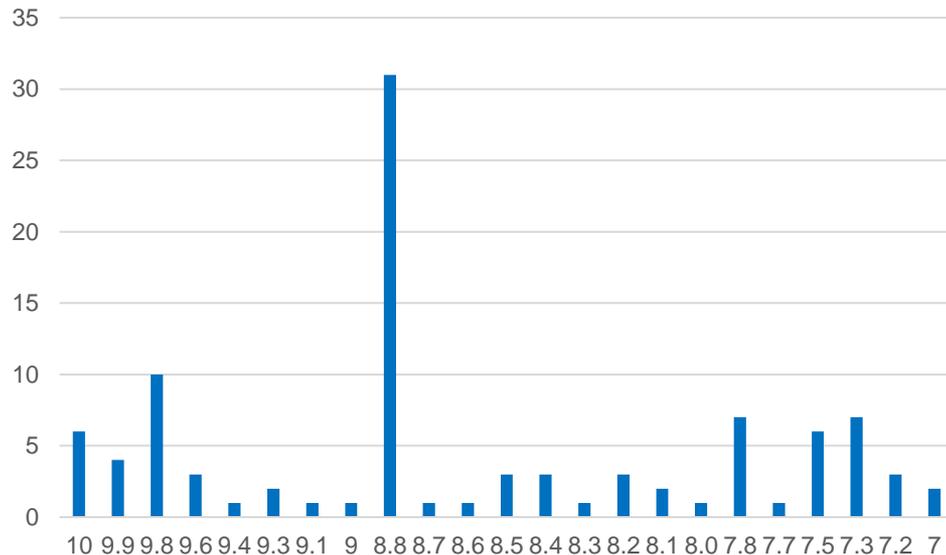


# Nombre de CVE par catégorie de produit et score CVSS

## CVE par catégorie de solution

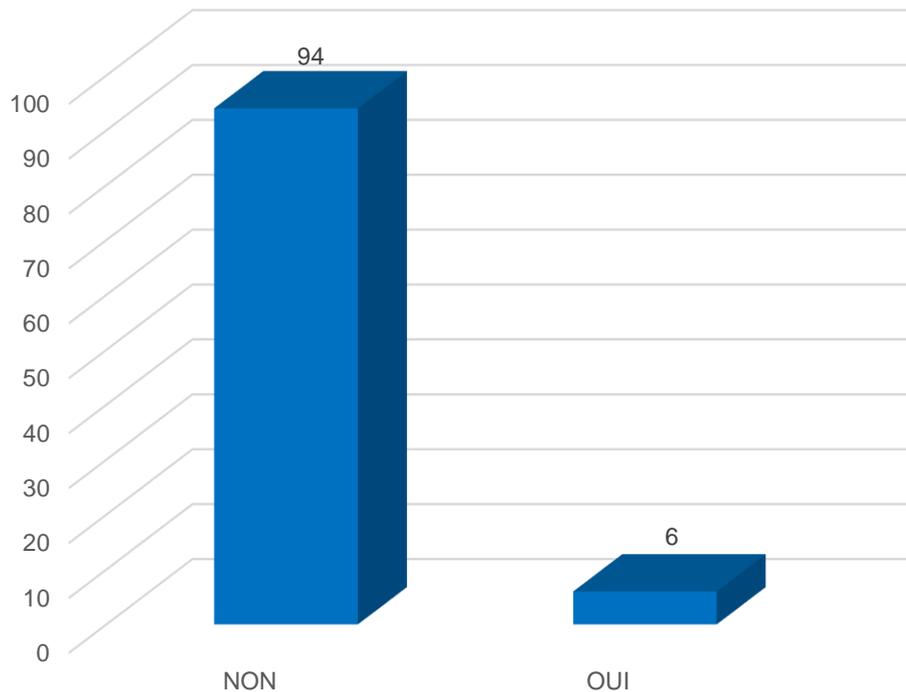


## CVE par score CVSS

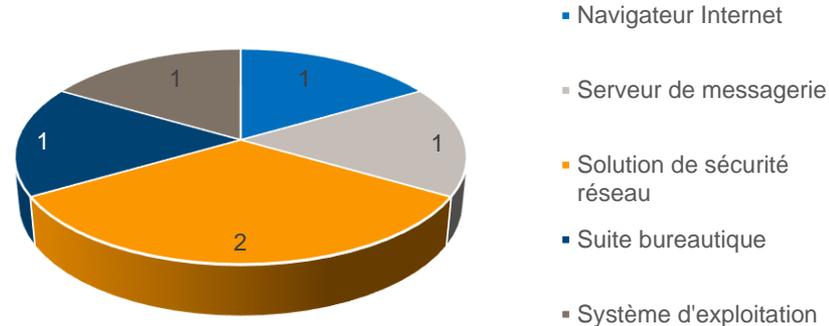


# Vulnérabilités exploitées

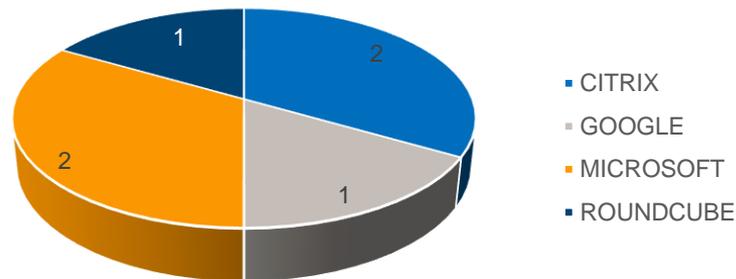
## Failles exploitées



## Failles exploitées par type de solution



## Failles exploitées par éditeur



# Les vulnérabilités critiques à surveiller

10 ▶

## Citrix

([CVE-2025-5777](#))

Atteinte à la confidentialité  
des données

Exploitée

Un défaut de vérification des données saisies par l'utilisateur dans l'interface d'administration de Citrix Netscaler permet à un attaquant, en envoyant des requêtes spécifiquement forgées, de porter atteinte à la confidentialité et à l'intégrité des données ou de provoquer un déni de service.

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

9.3 ▶

## Roundcube

([CVE-2024-42009](#))

Contournement de la  
politique de sécurité

Exploitée

Un défaut de contrôle des données saisies par les utilisateurs dans Roundcube permet à un attaquant non authentifié, en persuadant une victime de cliquer sur un courriel spécifiquement forgé, d'injecter du code (injection XSS). Celui-ci, exécuté dans le navigateur de la victime, permet d'usurper sa boîte de messagerie.

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

8.4 ▶

## Microsoft

([CVE-2025-47957](#))

Exécution de code arbitraire

Exploitée

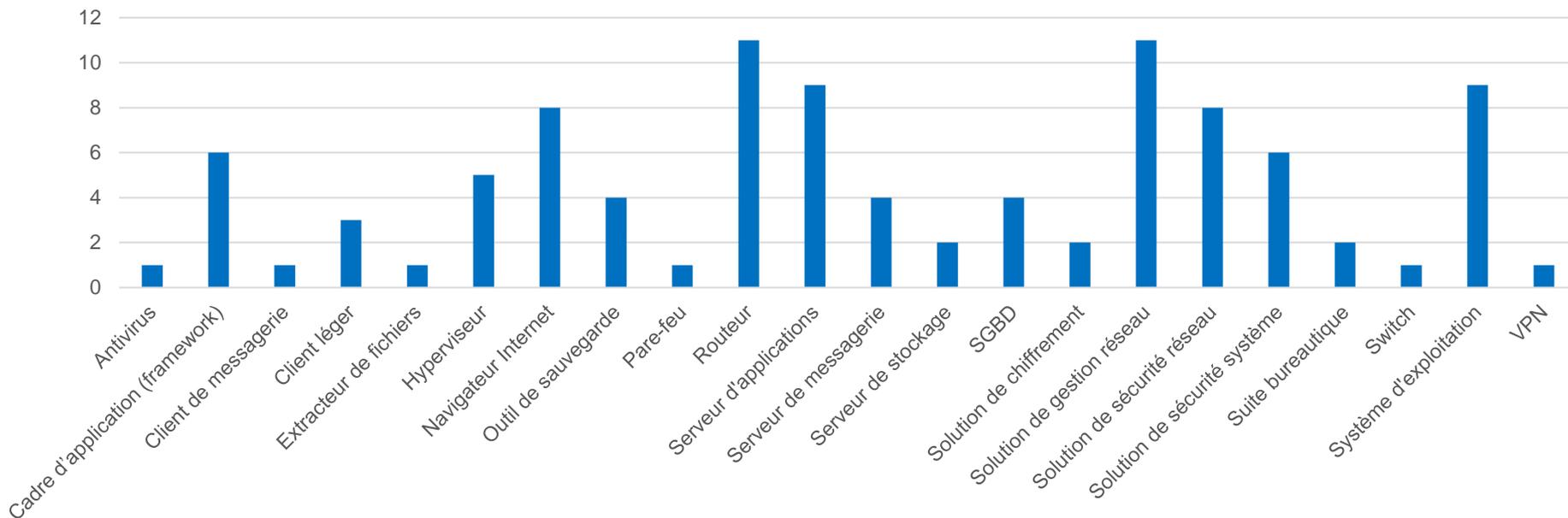
Un défaut de libération de la mémoire dans Microsoft Word permet à un attaquant non authentifié d'exécuter du code arbitraire sur le système.

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

## Types de solutions vulnérables

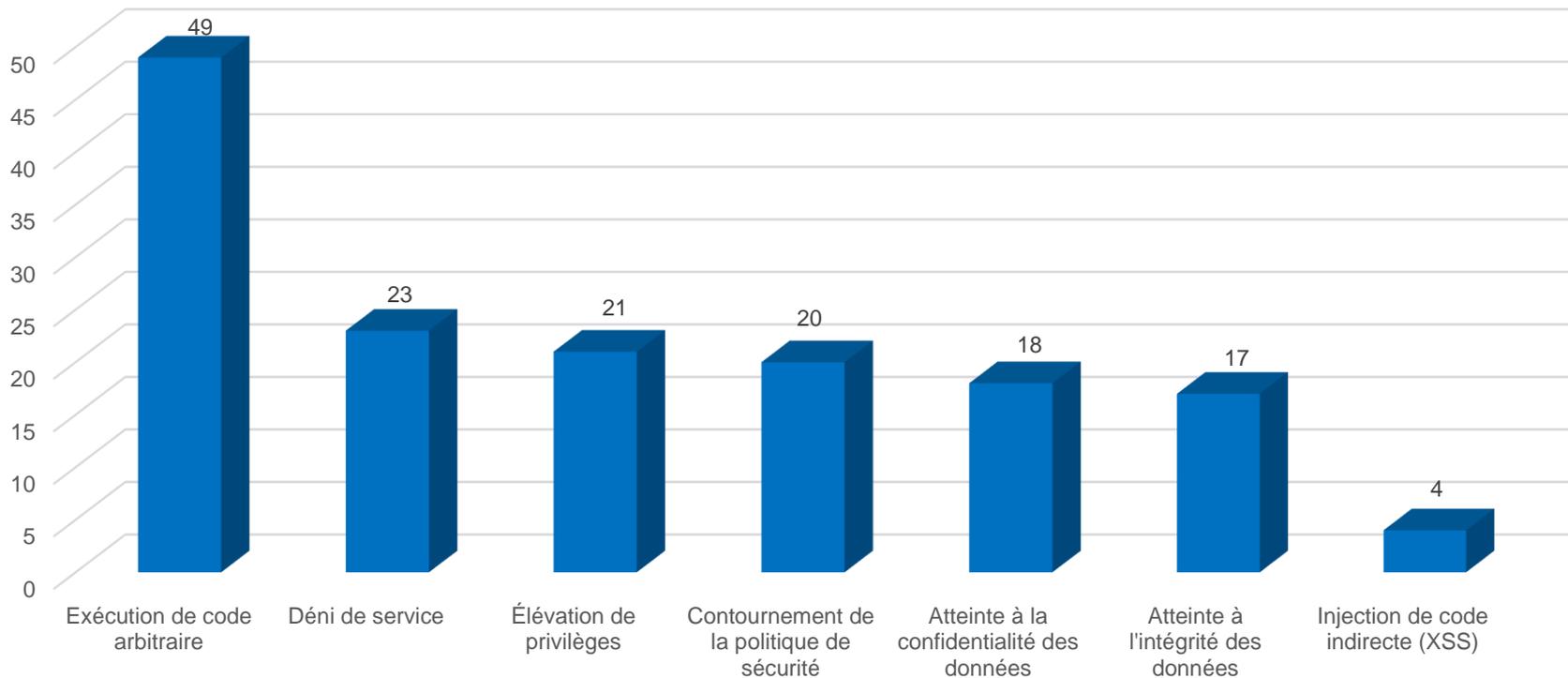
Les solutions de gestion réseau, les routeurs, les serveurs d'application et les systèmes d'exploitation sont les principaux types d'équipements affectés par les vulnérabilités publiées.

CVE par type de solution



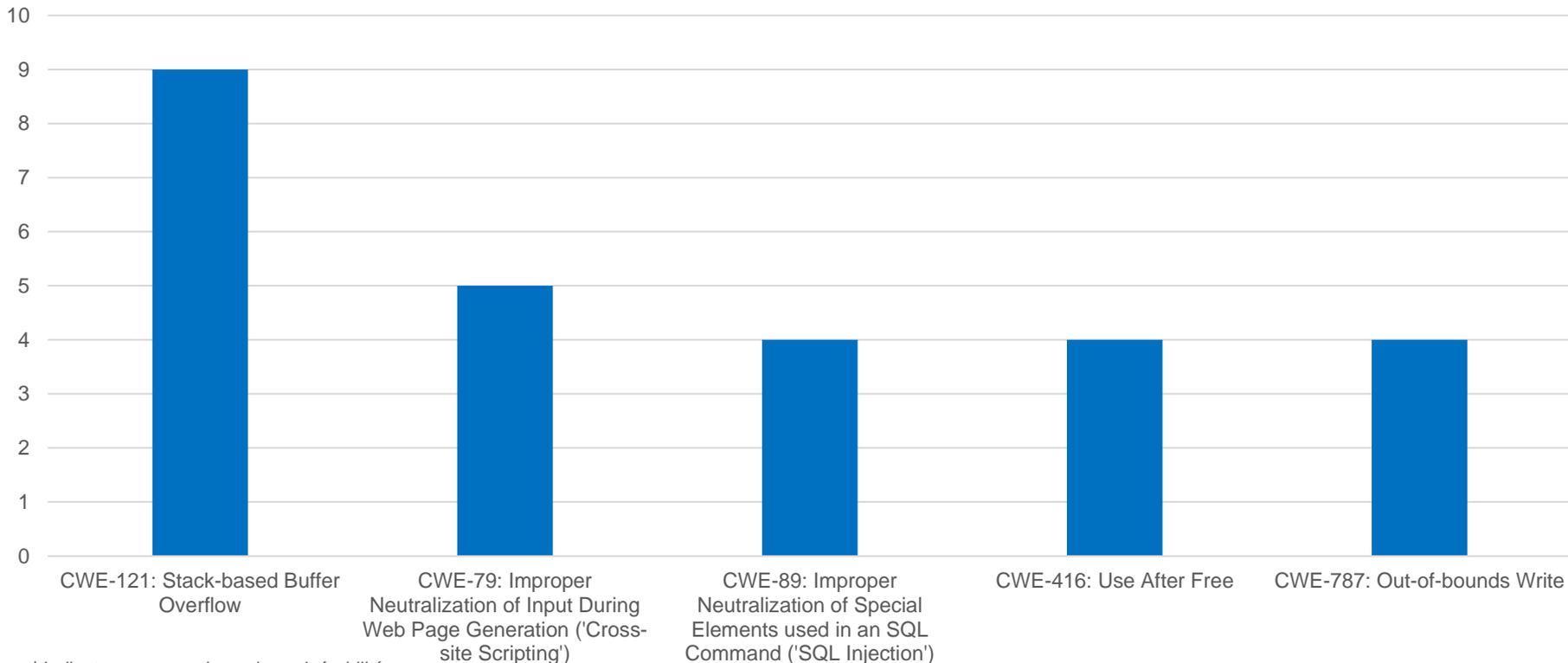
# Types de menaces

Type de menaces



# TOP 5 des failles selon le référentiel CWE

Nombre de CVE par CWE



| Indicateurs mensuels sur les vulnérabilités