



**AGENCE
DU NUMÉRIQUE
EN SANTÉ**

La transformation commence ici

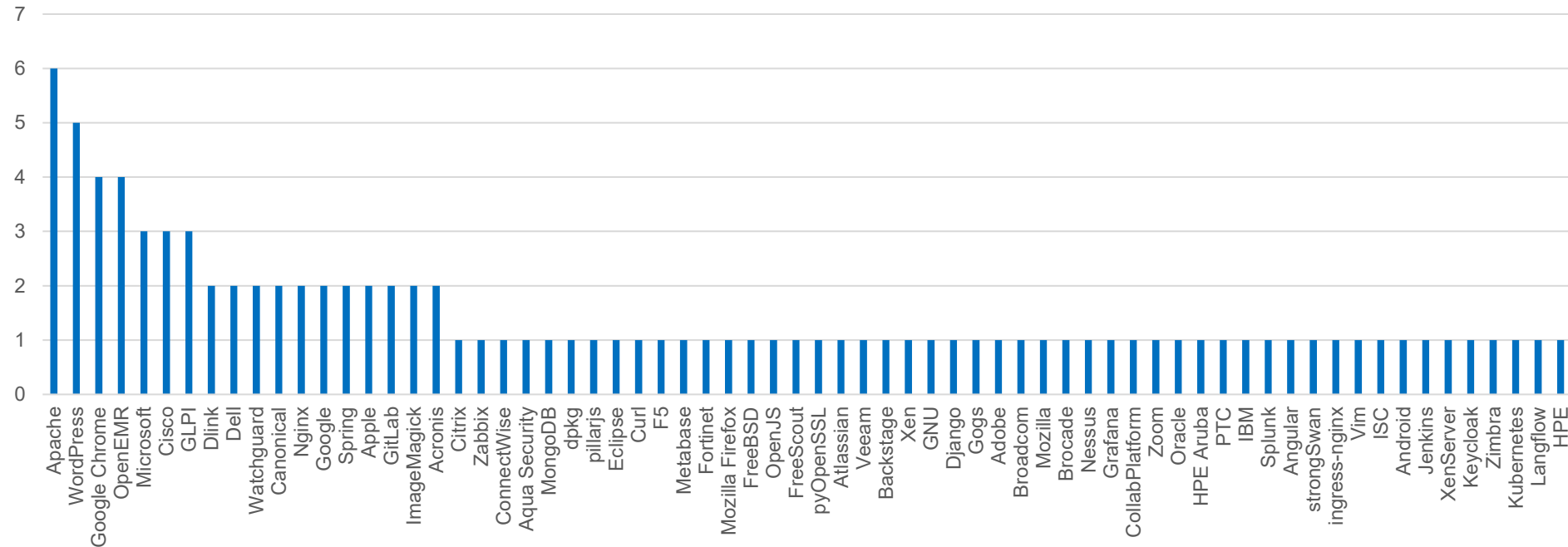


Indicateurs sur la publication des CVE pour le mois de mars 2026

Nombre de CVE par éditeur

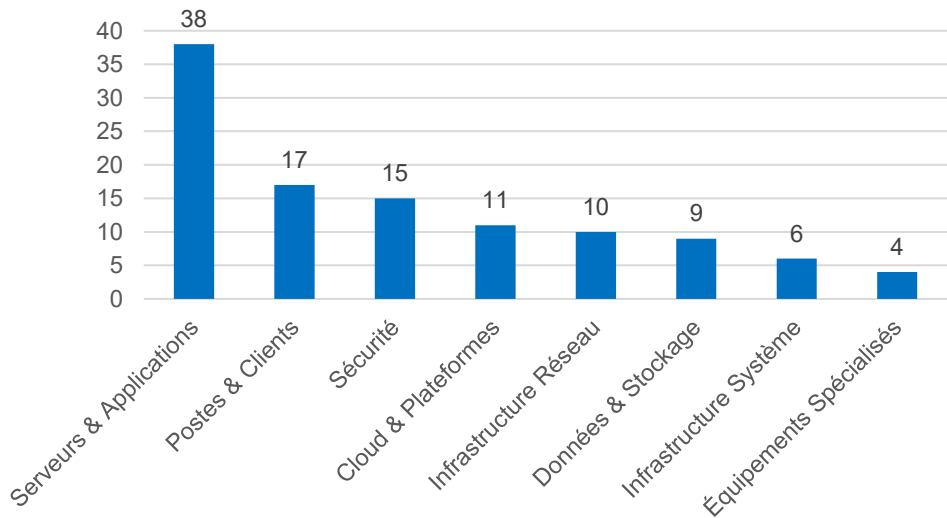
110 vulnérabilités ont été analysées et publiées (parmi lesquelles 7 alertes) sur le portail du CERT Santé.

CVE par éditeur

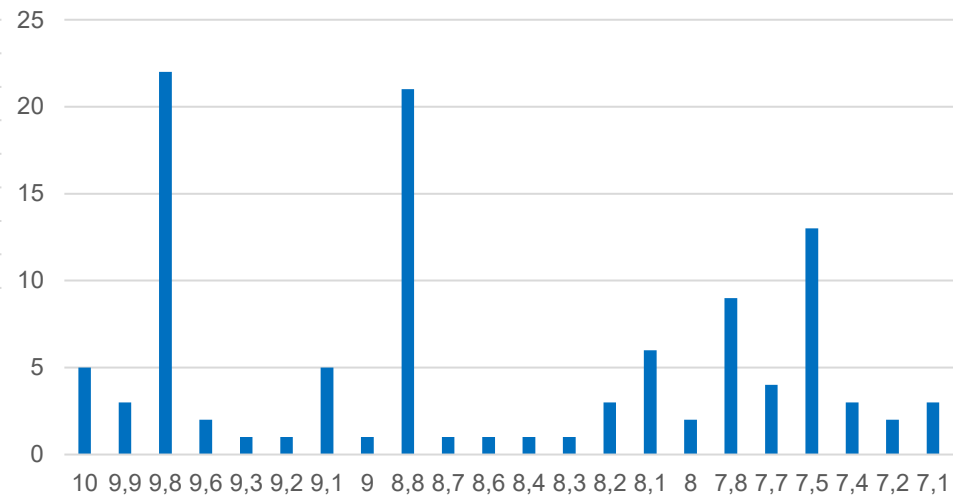


Nombre de CVE par catégorie de produit et score CVSS

CVE par catégorie de solution

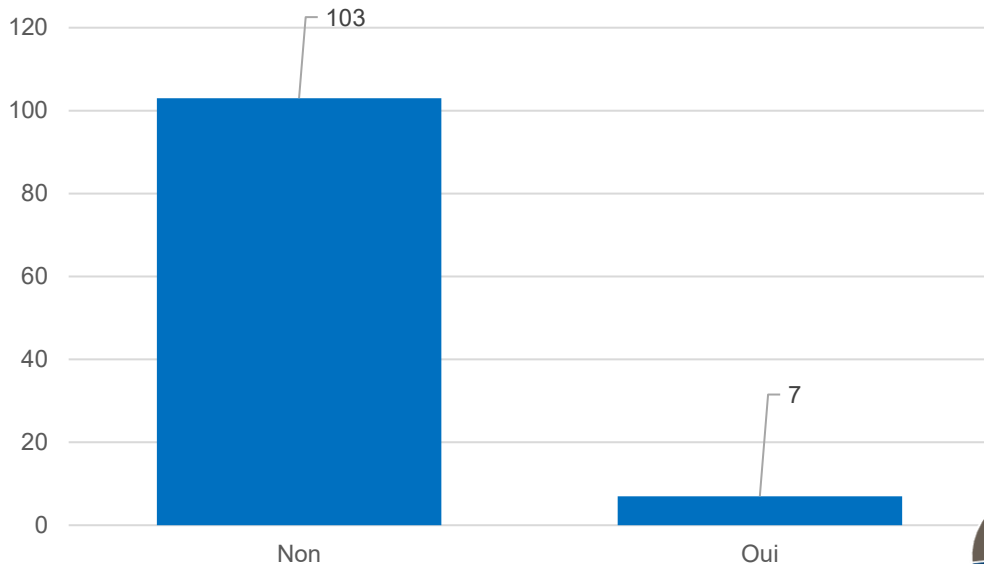


CVE par score CVSS

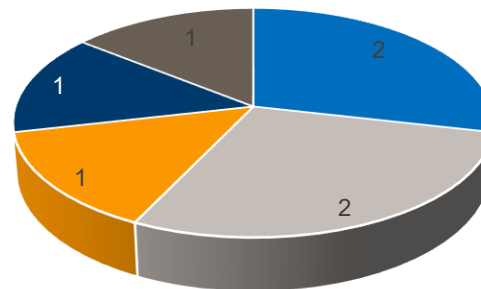


Vulnérabilités exploitées

Failles exploitées

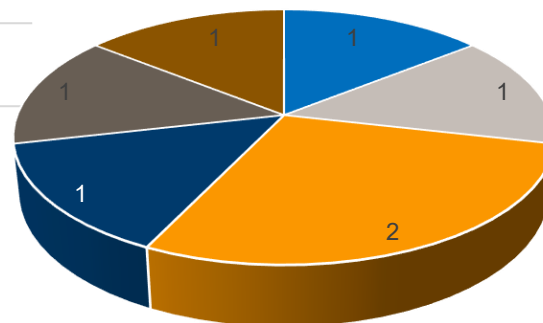


Failles exploitées par type de solution



- Navigateur Internet
- Outil DevOps / CI-CD / Automation
- Plugin / Extension CMS
- Serveur web / Application web
- Système d'exploitation

Failles exploitées par éditeur



- Android
- Aqua Security
- Google Chrome
- Langflow AI
- PTC
- WordPress

Les vulnérabilités critiques à surveiller

8.8

Trivy

([CVE-2026-33634](#))

Exécution de code arbitraire

Exploitée

L'exploitation d'une vulnérabilité de **supply chain** dans Trivy permet l'**injection de code malveillant** dans des **pipelines CI/CD**, entraînant **une exécution de code à distance** et l'**exfiltration de secrets (tokens cloud, clés SSH, credentials)**.

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

10

Windchill

([CVE-2026-4681](#))

Elévation de privilèges

Exploitée

L'exploitation d'une vulnérabilité de **désérialisation non sécurisée** dans Windchill permet une **exécution de code à distance sans authentification** via des requêtes HTTP malveillantes, entraînant une **compromission complète du serveur** et un **accès aux données sensibles industrielles**.

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

9.8

Langflow AI

([CVE-2026-33017](#))

Exécution de code arbitraire

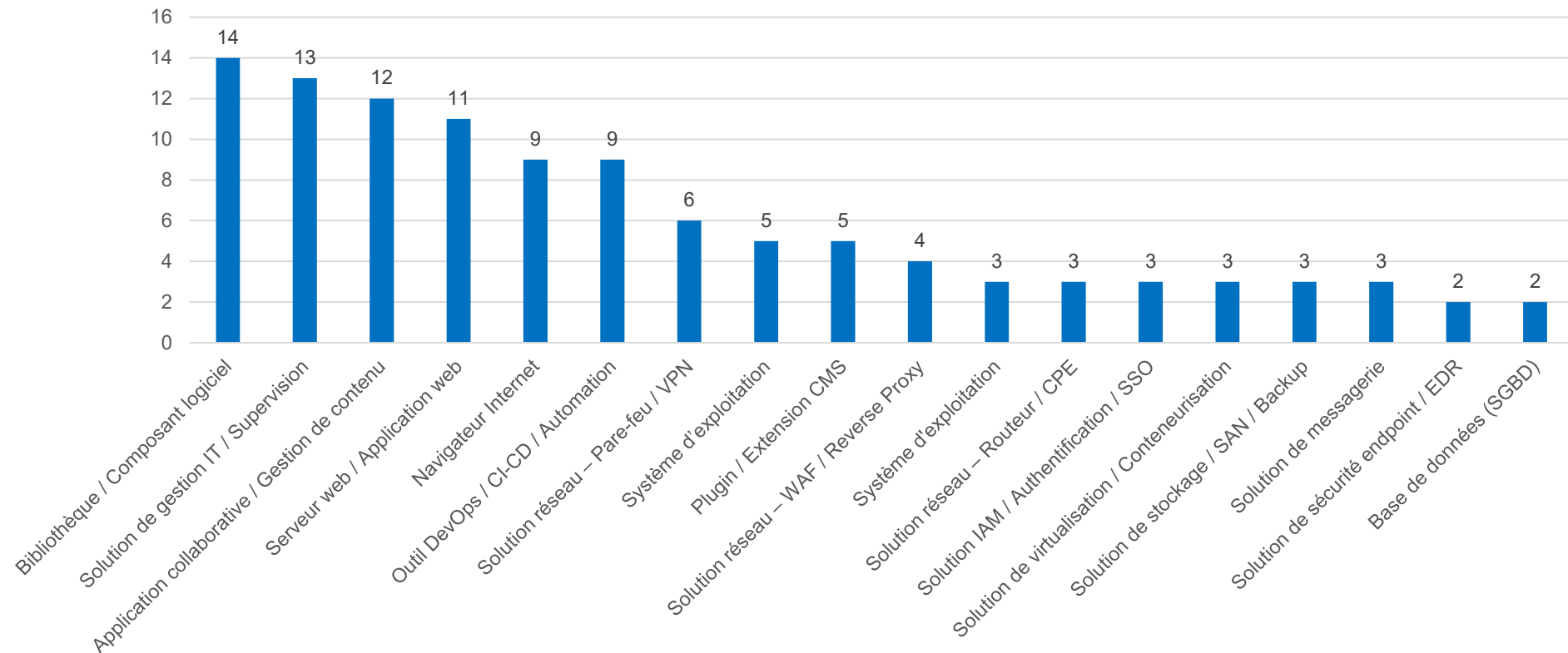
Exploitée

L'exploitation d'une vulnérabilité **d'absence d'authentification** dans Langflow permet l'**exécution de code arbitraire** via un endpoint public utilisant **exec()**, entraînant une **compromission complète du serveur** et l'**exfiltration de secrets (clés API, tokens, identifiants)**.

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

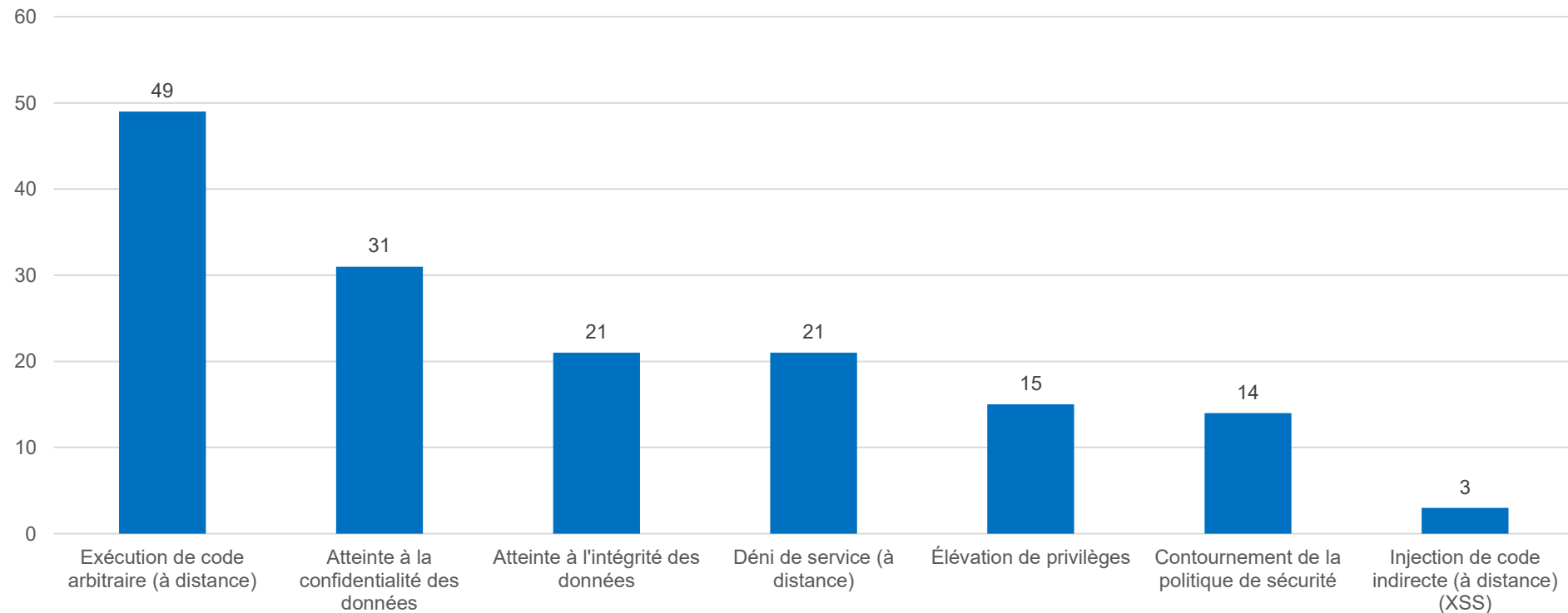
Types de solutions vulnérables

CVE par type de solution



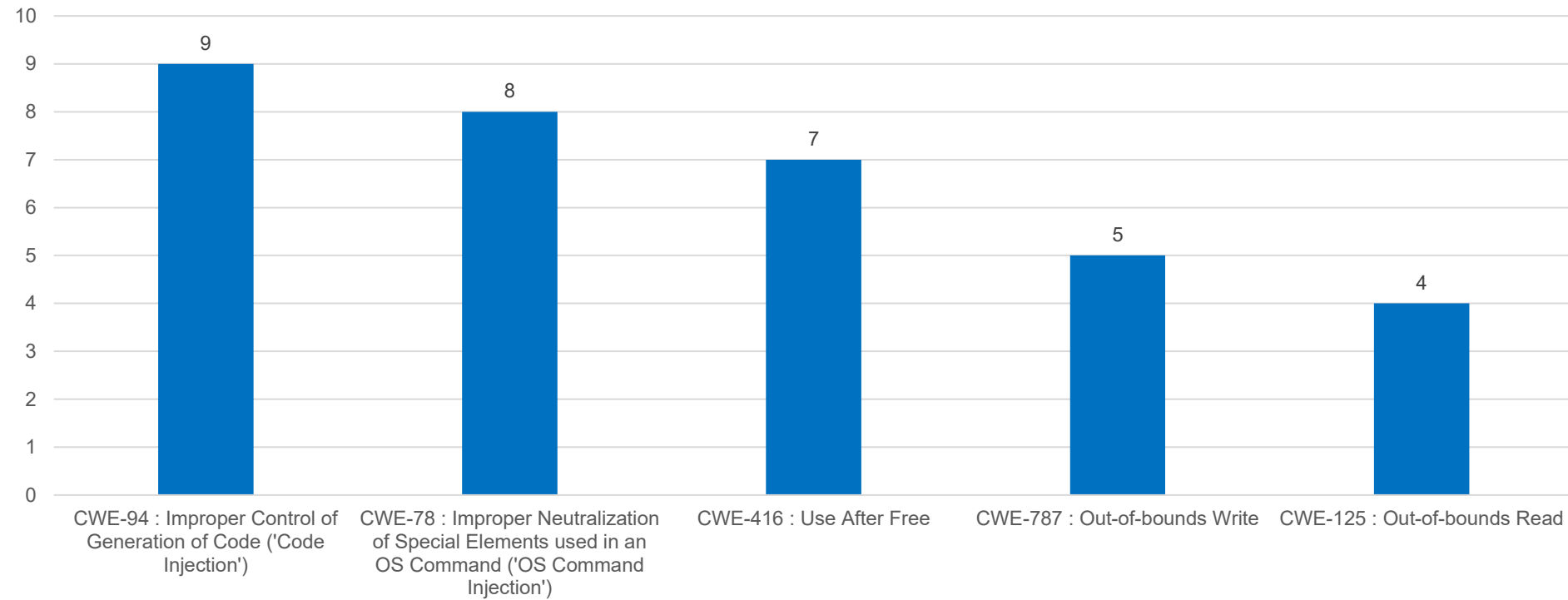
Types de menaces

Types de menaces



TOP 5 des failles selon le référentiel CWE

Nombre de CVE par CWE



| Indicateurs mensuels sur les vulnérabilités