CERT Santé

LA E-SANTÉ FRANÇAISE

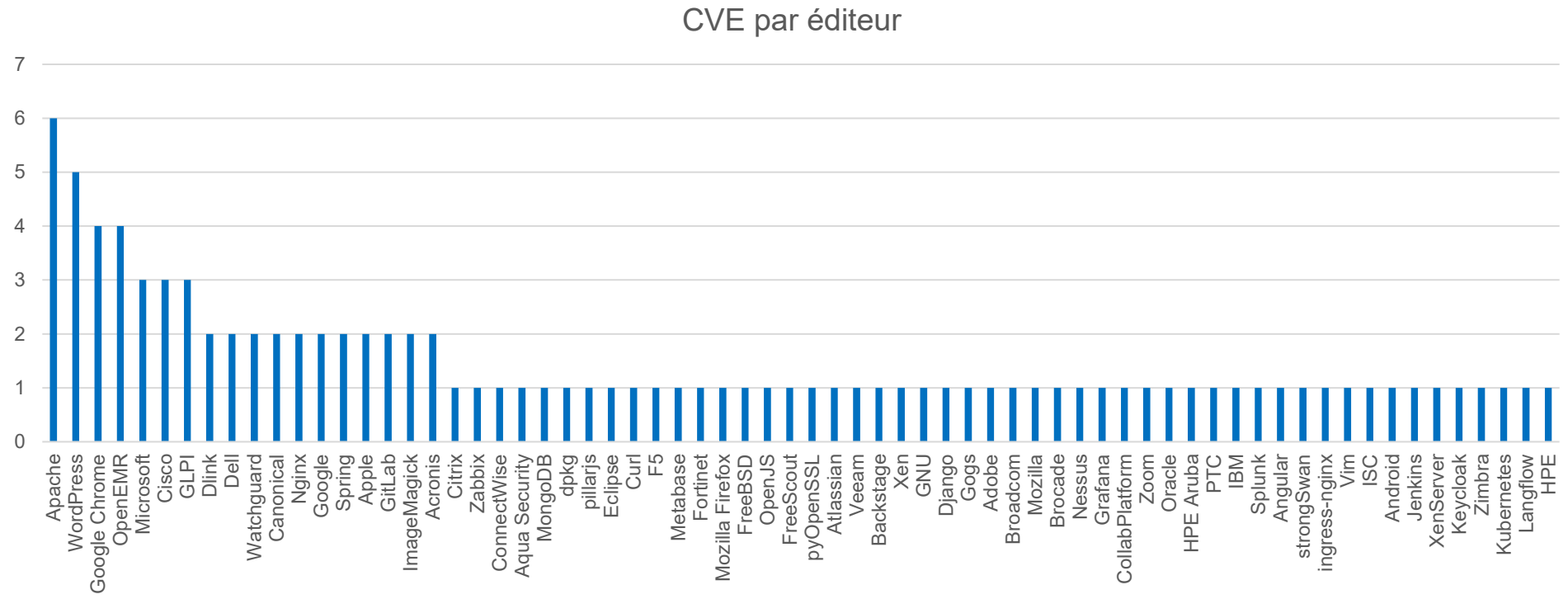
AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

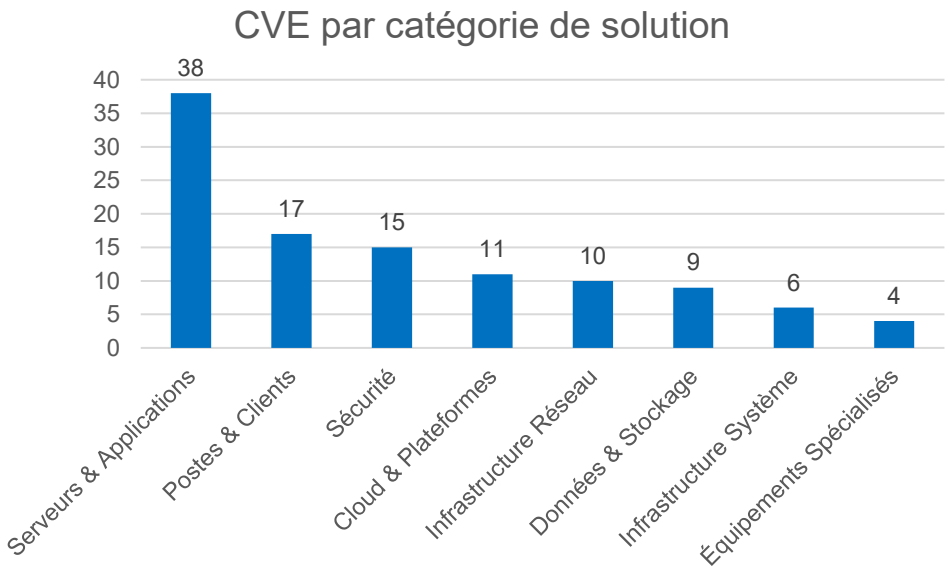
Indicateurs sur la publication des CVE pour le mois de mars 2026

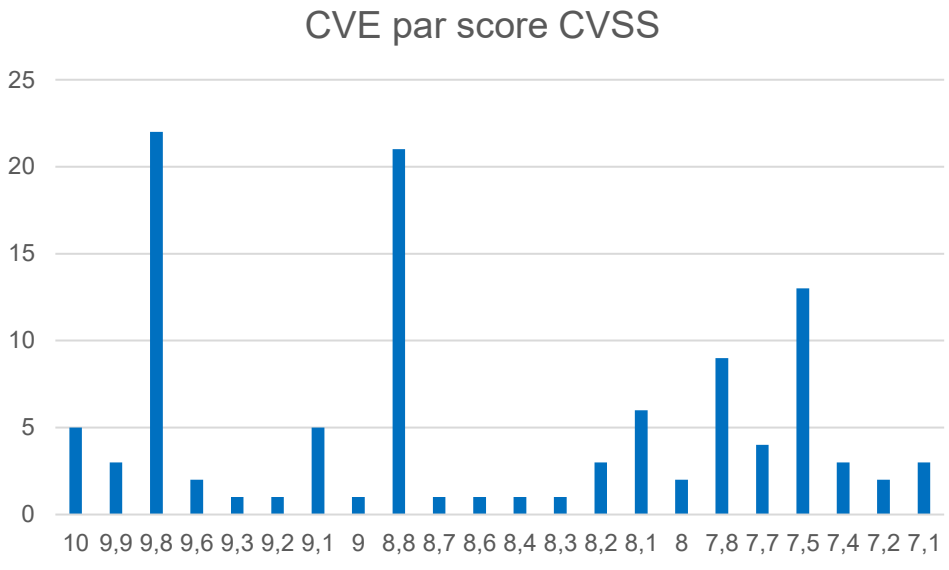
Nombre de CVE par éditeur

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

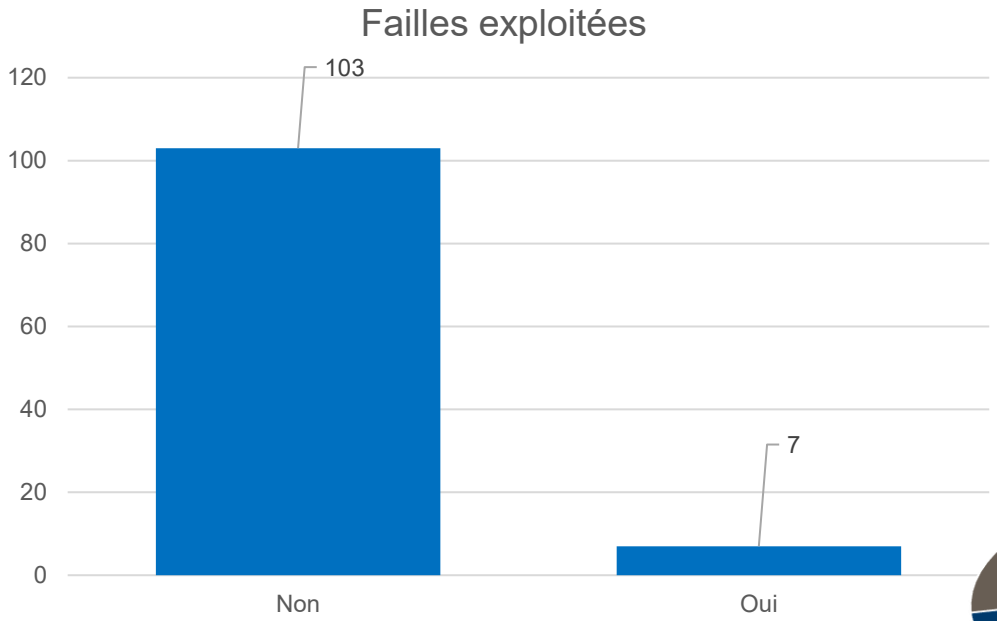


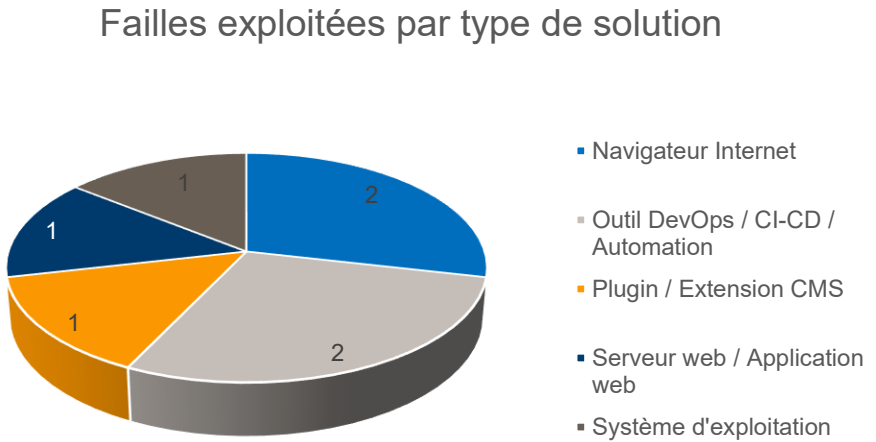
Nombre de CVE par catégorie de produit et score CVSS

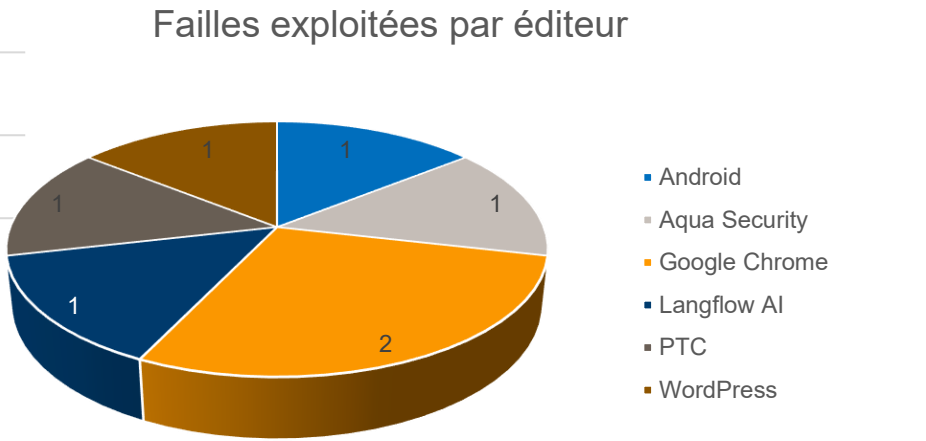




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

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.

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.

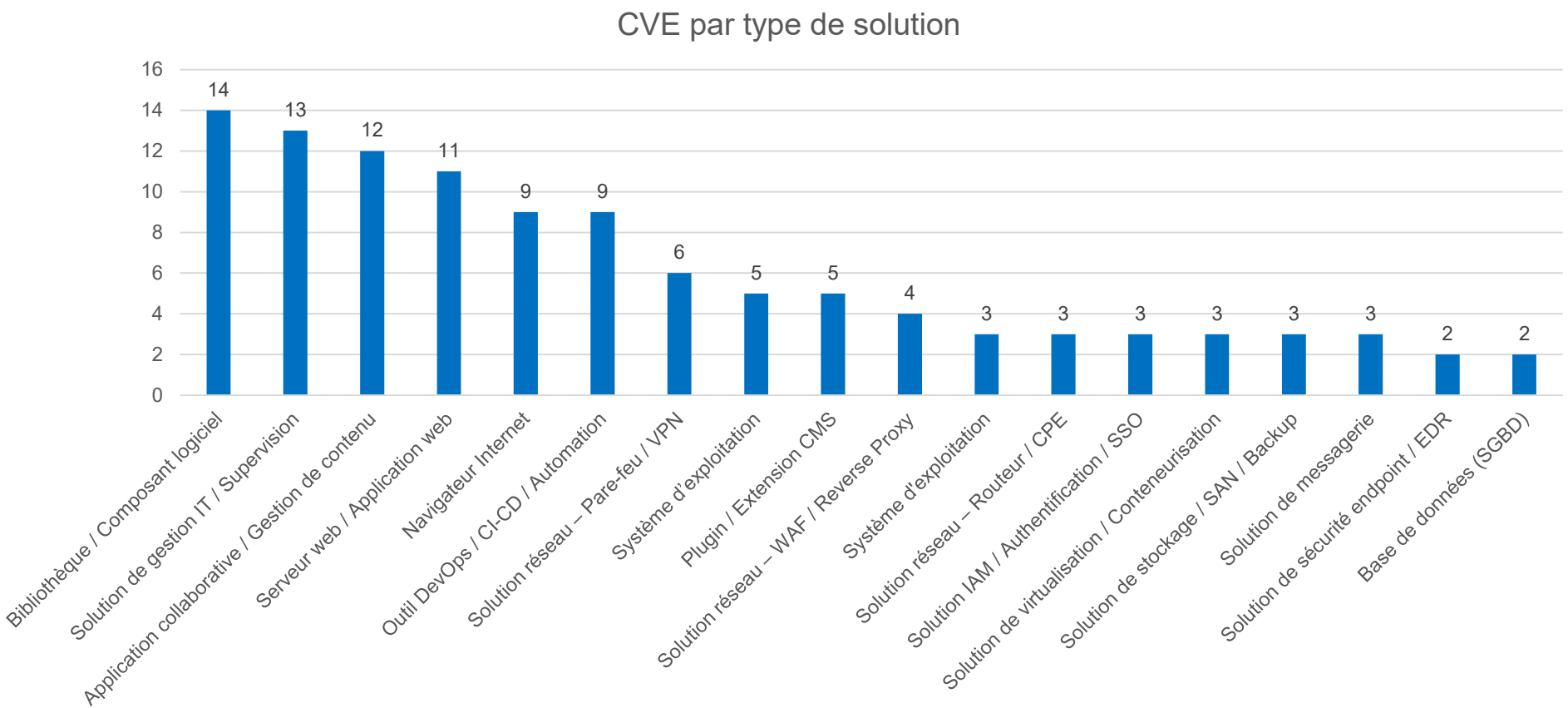
Langflow AI
(CVE-2026-33017)

Exécution de code arbitraire | Exploitée

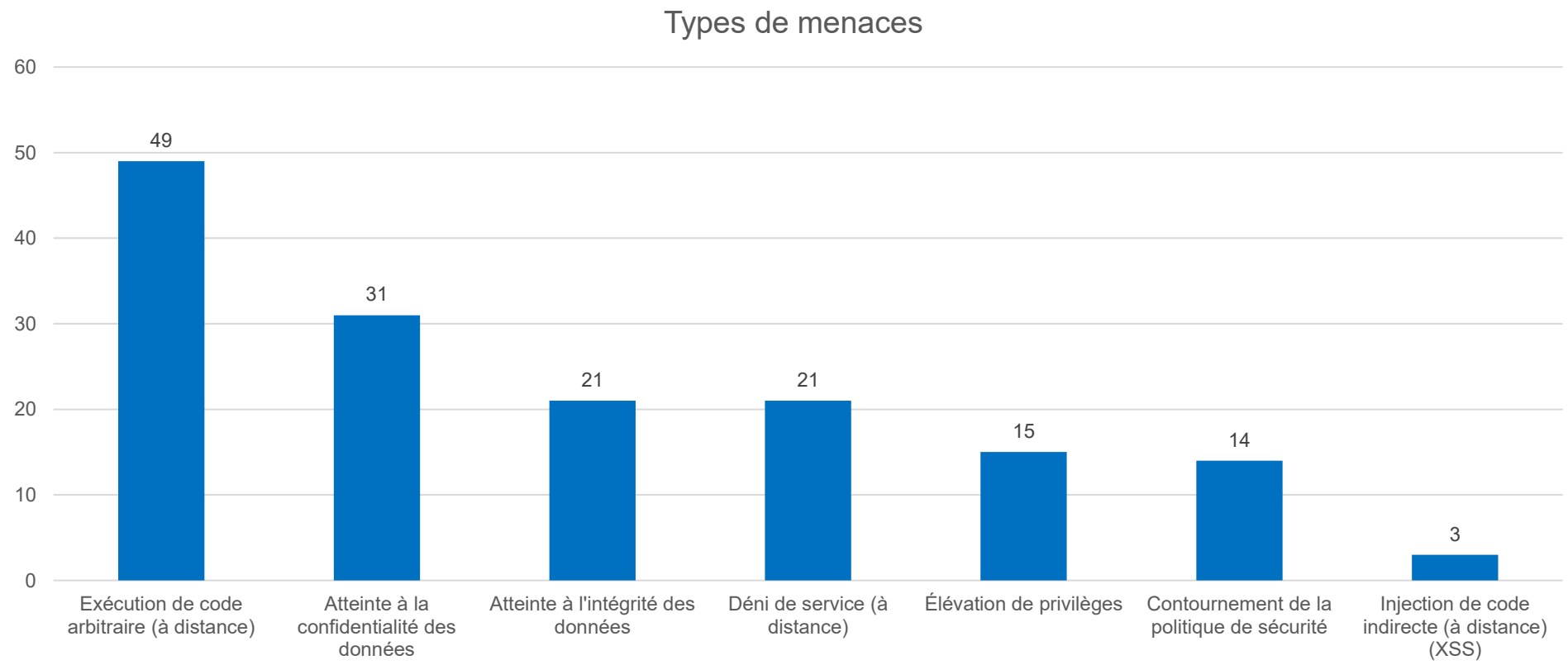
L'exploitation d'une vulnérabilité **d'absence d'authentification** dans Langflow permet **l'exécution de code arbitraire** via un endpoint public utilisant **exec(),** entraînant une **compromission complète du serveur** et **l'exfiltration de secrets (clés API, tokens, identifiants).**

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

Types de solutions vulnérables



Types de menaces



TOP 5 des failles selon le référentiel CWE