CERT Santé

LA E-SANTÉ FRANÇAISE

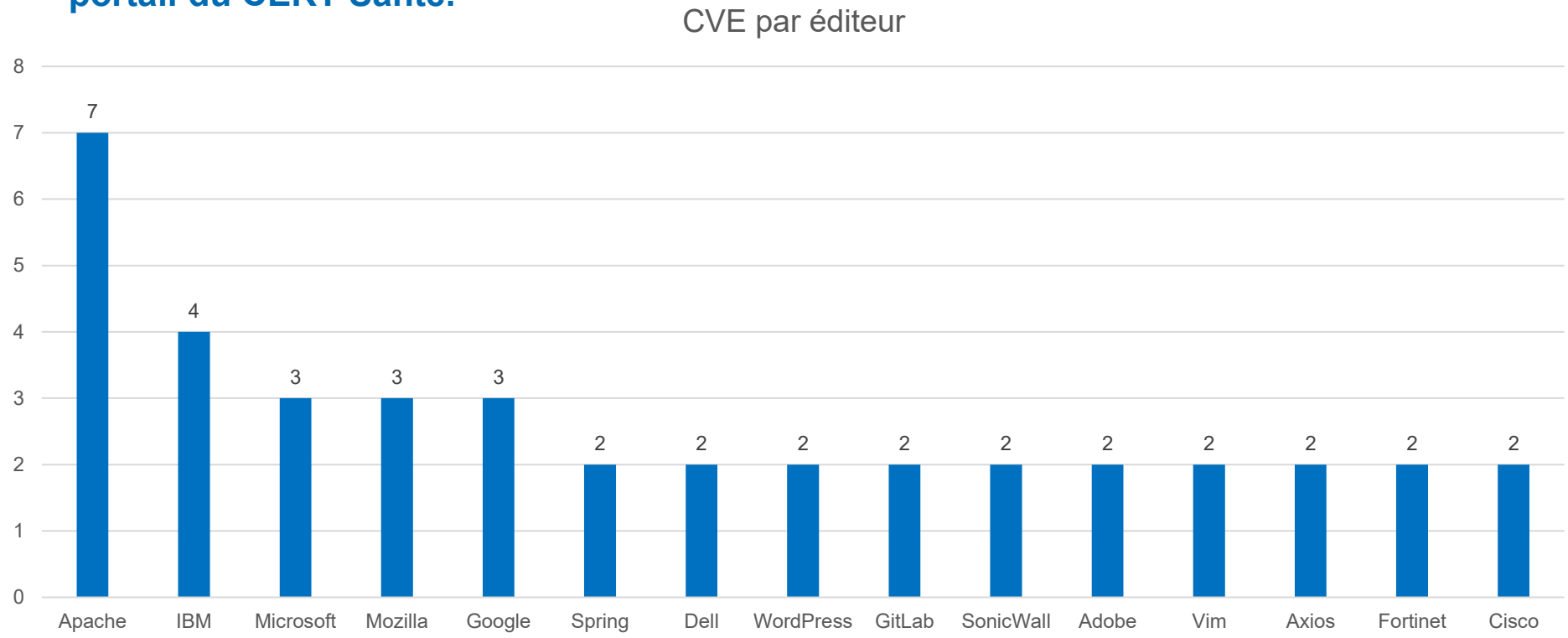
AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

Indicateurs sur la publication des CVE pour le mois d’avril 2026

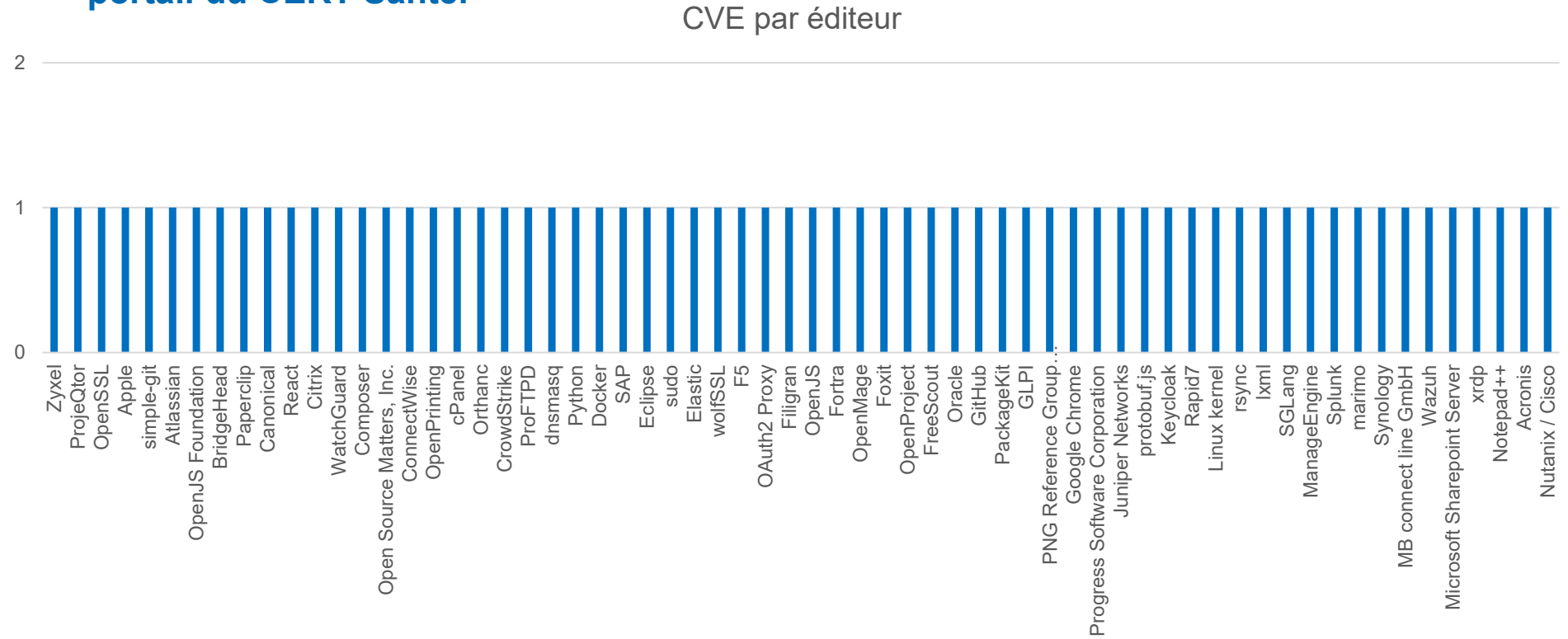
Nombre de CVE par éditeur

104 vulnérabilités ont été analysées et publiées (parmi lesquelles 10 alertes) sur le portail du CERT Santé.

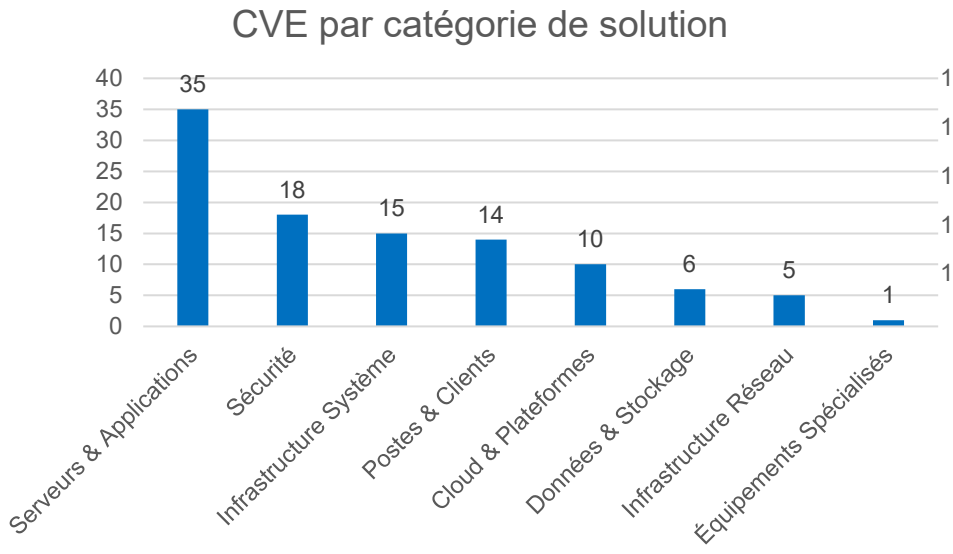


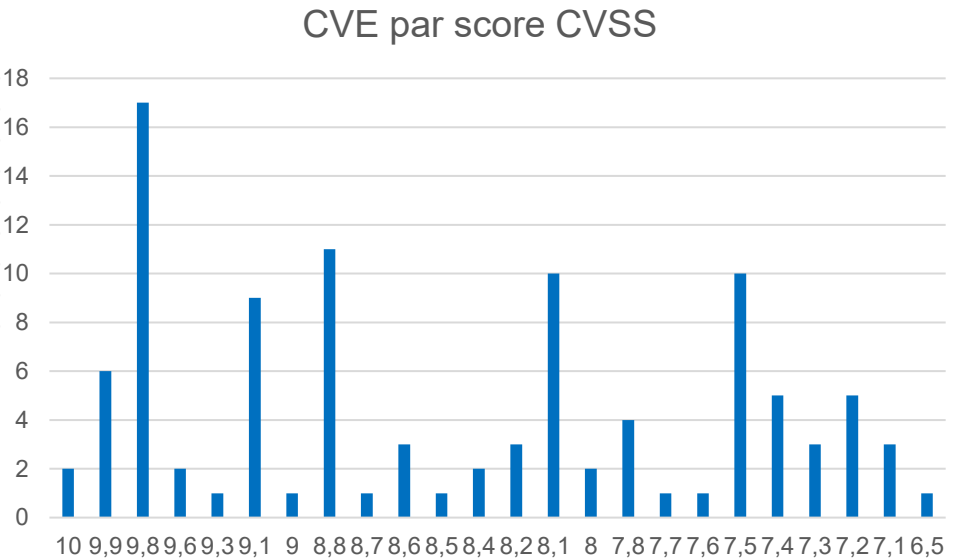
Nombre de CVE par éditeur

104 vulnérabilités ont été analysées et publiées (parmi lesquelles 10 alertes) sur le portail du CERT Santé.

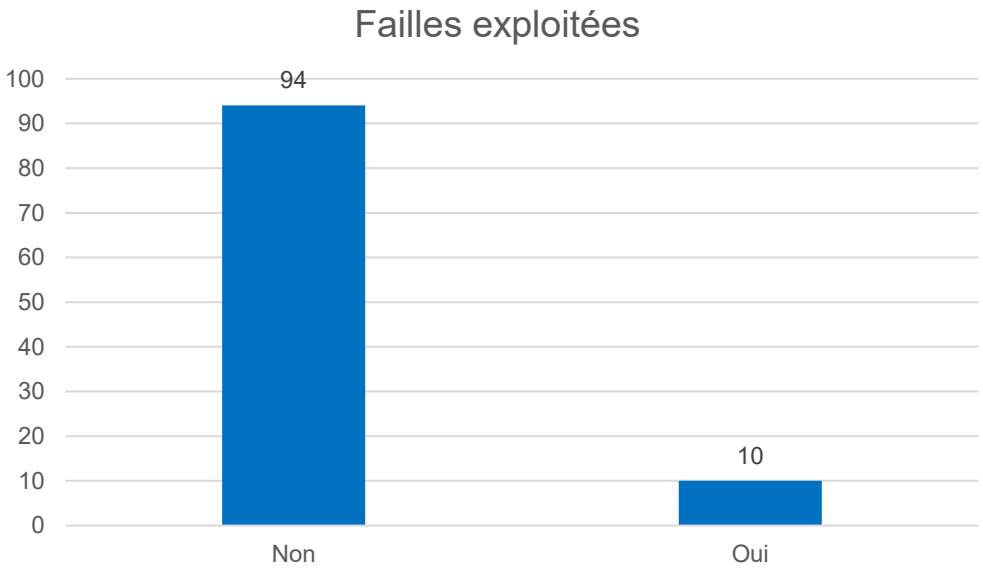


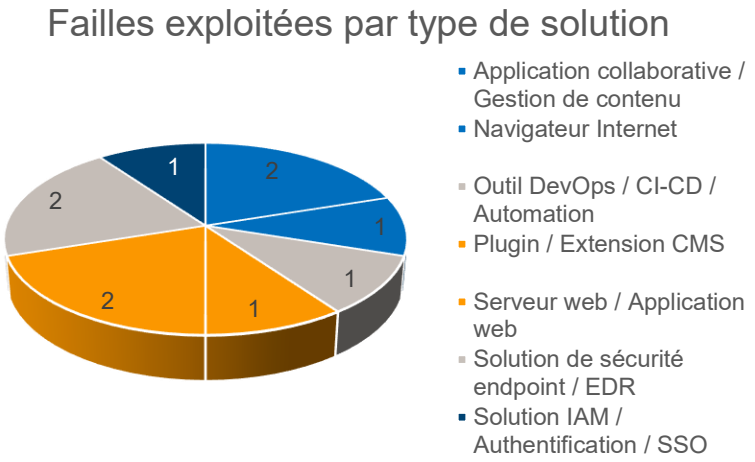
Nombre de CVE par catégorie de produit et score CVSS

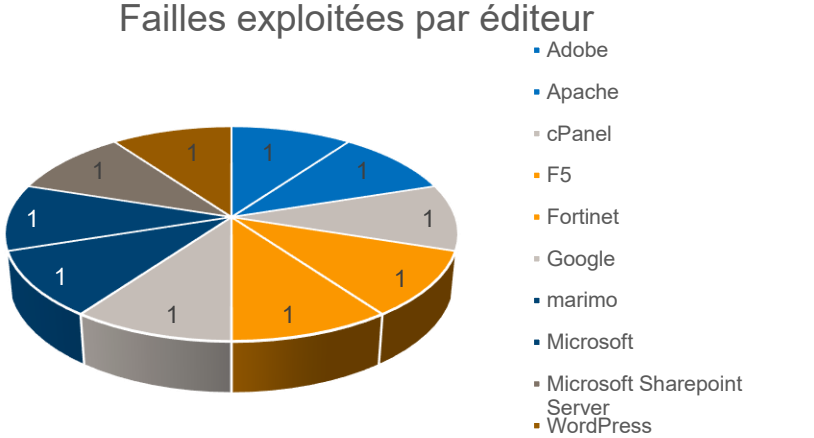




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

9.8

FortiClient EMS
(CVE-2026-35616)

Elévation de privilèges | Exploitée

L'exploitation d'une vulnérabilité de **contrôle d'accès incorrect** dans l'**API de FortiClient EMS** permet à un attaquant **distant non authentifié** d'exécuter du **code arbitraire** sur le **serveur de gestion**, entraînant une **compromission complète** de l'ensemble des **endpoints gérés** et des **politiques de sécurité** associées.

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

7.8

Microsoft Defender
(CVE-2026-33825)

Elévation de privilèges | Exploitée

L'exploitation d'une vulnérabilité de type **TOCTOU** dans la **plateforme anti-programme malveillant de Microsoft Defender** permet à un attaquant local de détourner les opérations de remédiation via un **oplock batch** et une **jonction NTFS**, entraînant une exécution de code arbitraire avec des **privilèges SYSTEM** et la **neutralisation de la protection du poste**. #BlueHammer

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

8.8

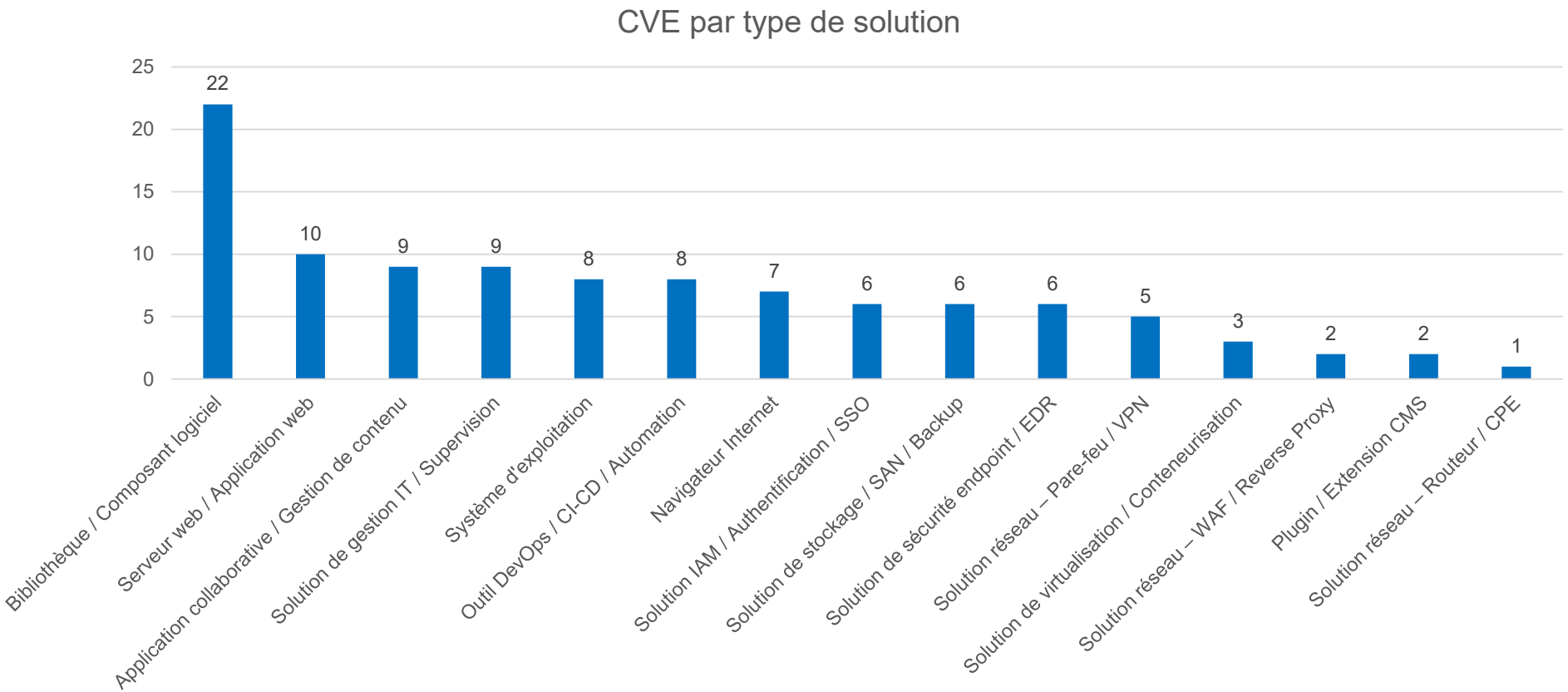
Apache ActiveMQ
(CVE-2026-34197)

Exécution de code arbitraire | Exploitée

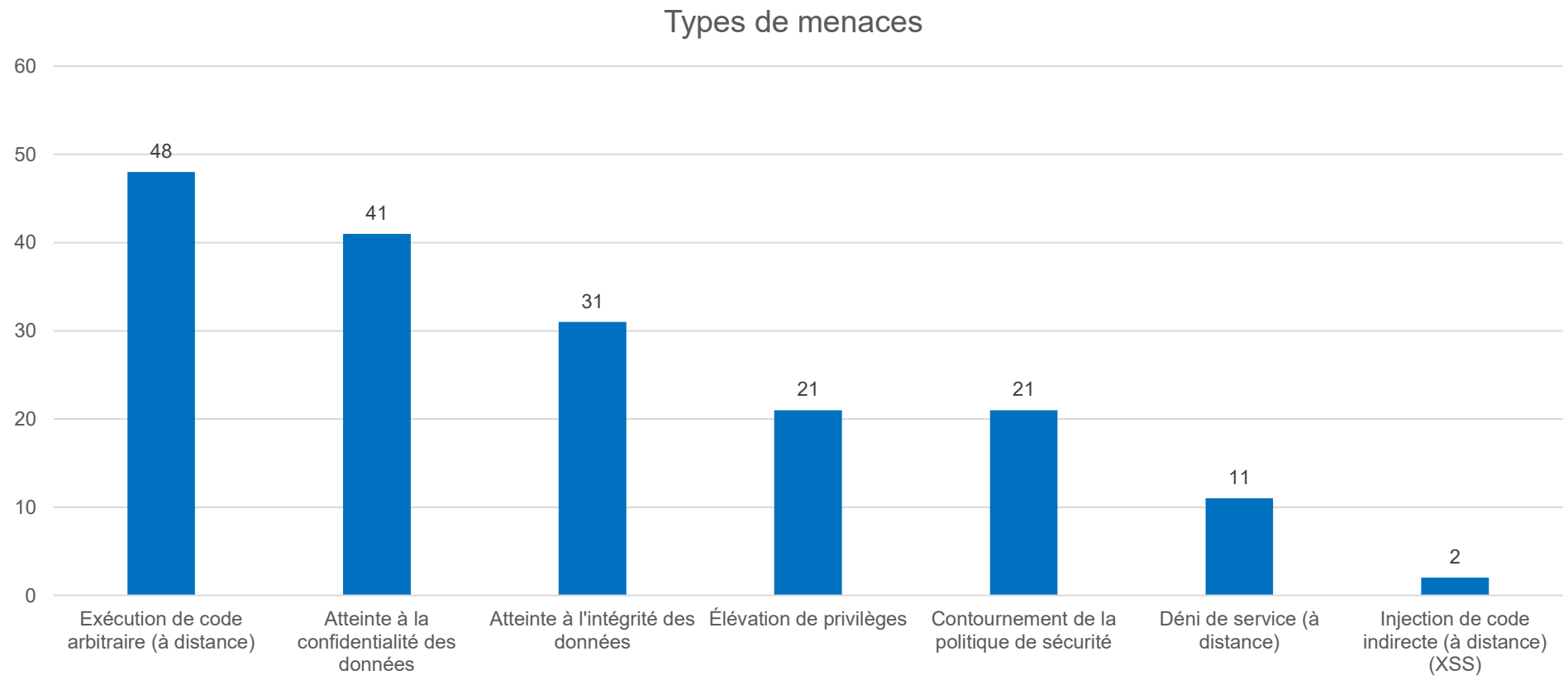
L'exploitation d'une vulnérabilité de **validation insuffisante des entrées** dans le **bridge JMX-HTTP Jolokia** d'**Apache ActiveMQ Classic** permet à un attaquant authentifié de déclencher l'instanciation de **beans Spring distants arbitraires**, entraînant une **exécution de code à distance** avec les droits du **processus broker** et une potentielle interruption des **flux d'interopérabilité**.

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 (7 CWE)