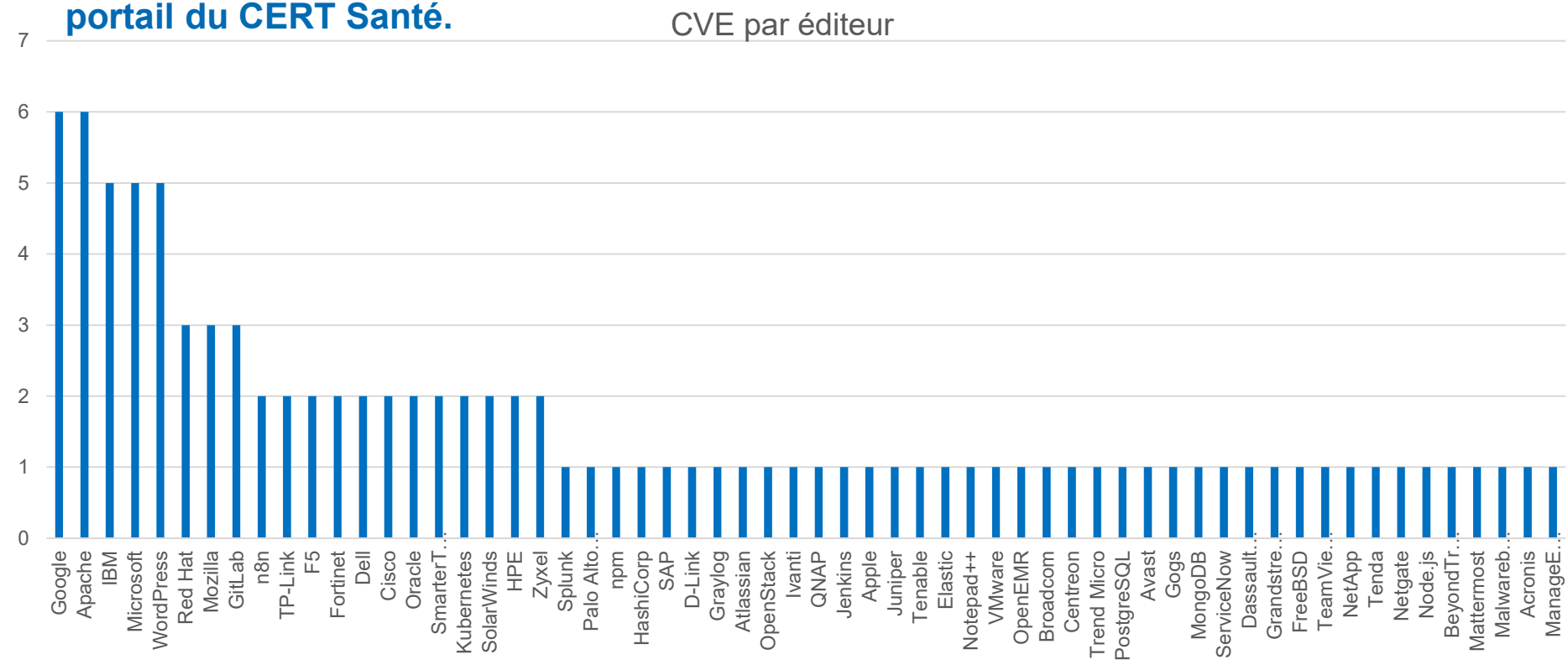
CERT Santé

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

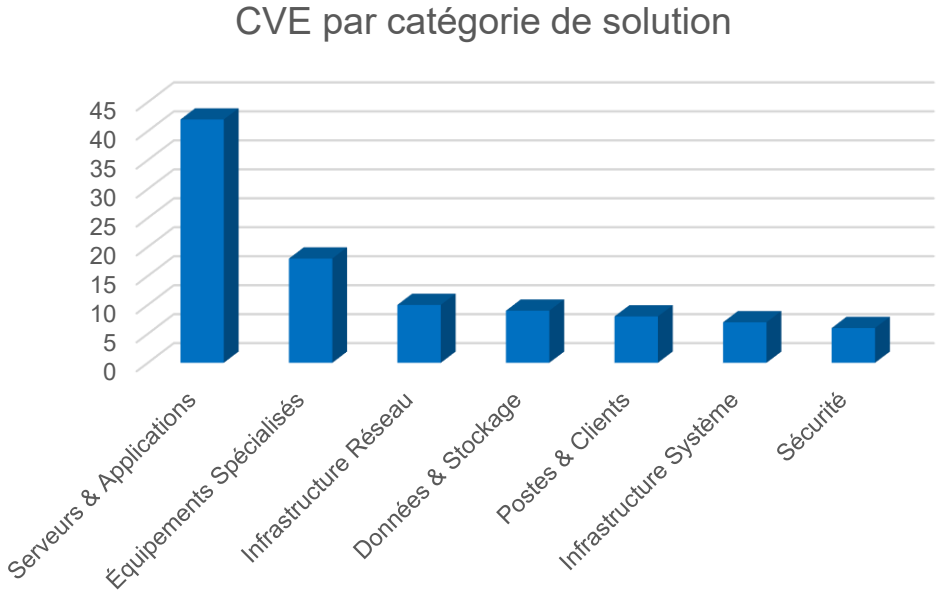
Indicateurs sur la publication des CVE pour le mois de février 2026

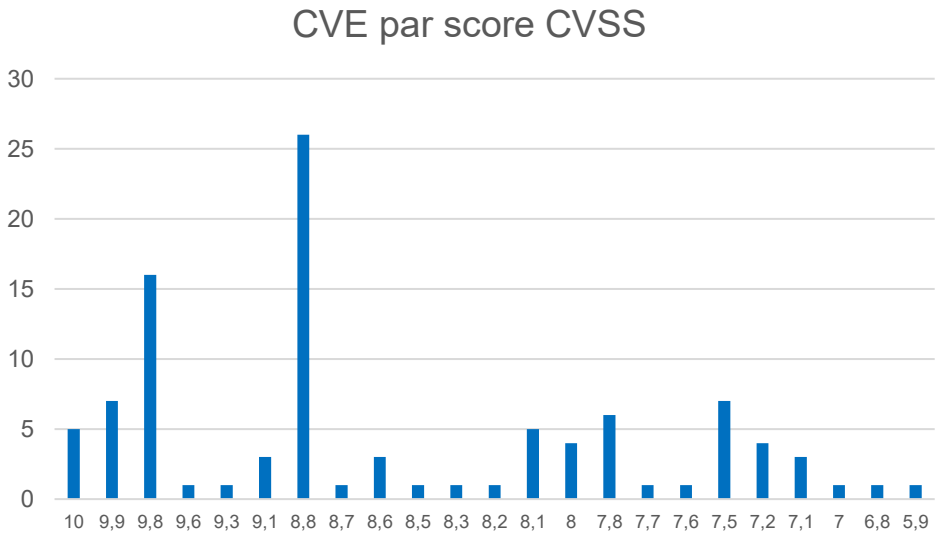
Nombre de CVE par éditeur

101 vulnérabilités ont été analysées et publiées (parmi lesquelles 9 alertes) sur le portail du CERT Santé.



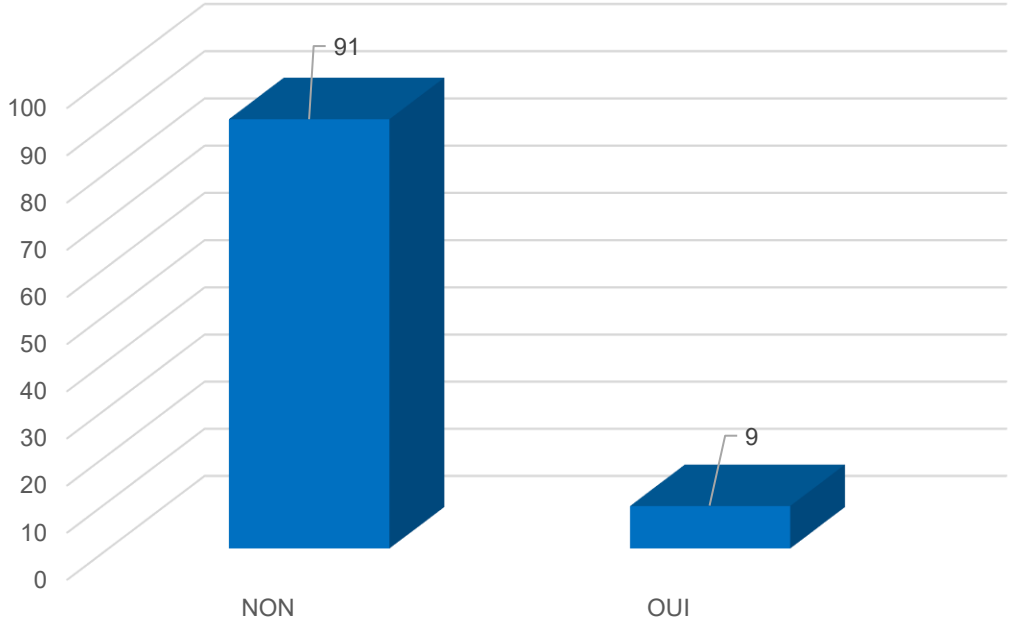
Nombre de CVE par catégorie de produit et score CVSS



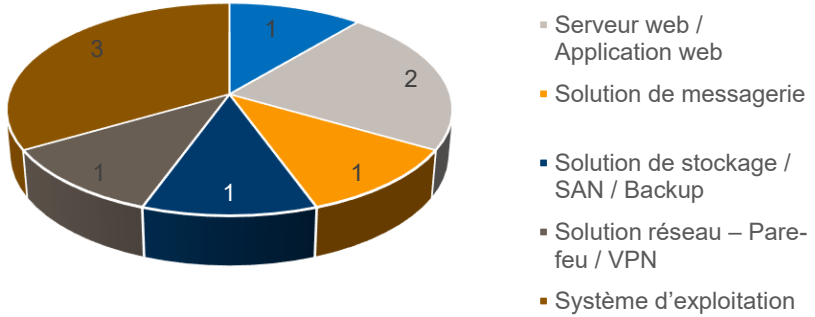


Vulnérabilités exploitées

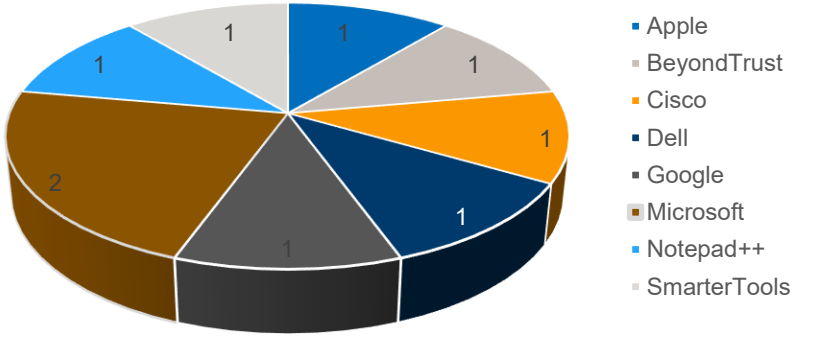
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

10

BeyondTrust
([CVE-2026-1731])

Exécution de code arbitraire | Exploitée

L'exploitation d'une **injection de commande** système pré-authentification. Un attaquant distant non authentifié peut envoyer des requêtes spécialement conçues afin d'**exécuter des commandes système** dans le contexte de l'utilisateur du site.

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

10

Cisco
(CVE-2026-20127)

Elévation de privilèges | Exploitée

L'exploitation d'une vulnérabilité d'authentification de peering sur Cisco Catalyst SD-WAN permet à un attaquant distant non authentifié de contourner l'authentification via des requêtes forgées et d'obtenir un accès administratif à un compte interne très privilégié, donnant accès à NETCONF pour manipuler la configuration du fabric SD-WAN

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

9.8

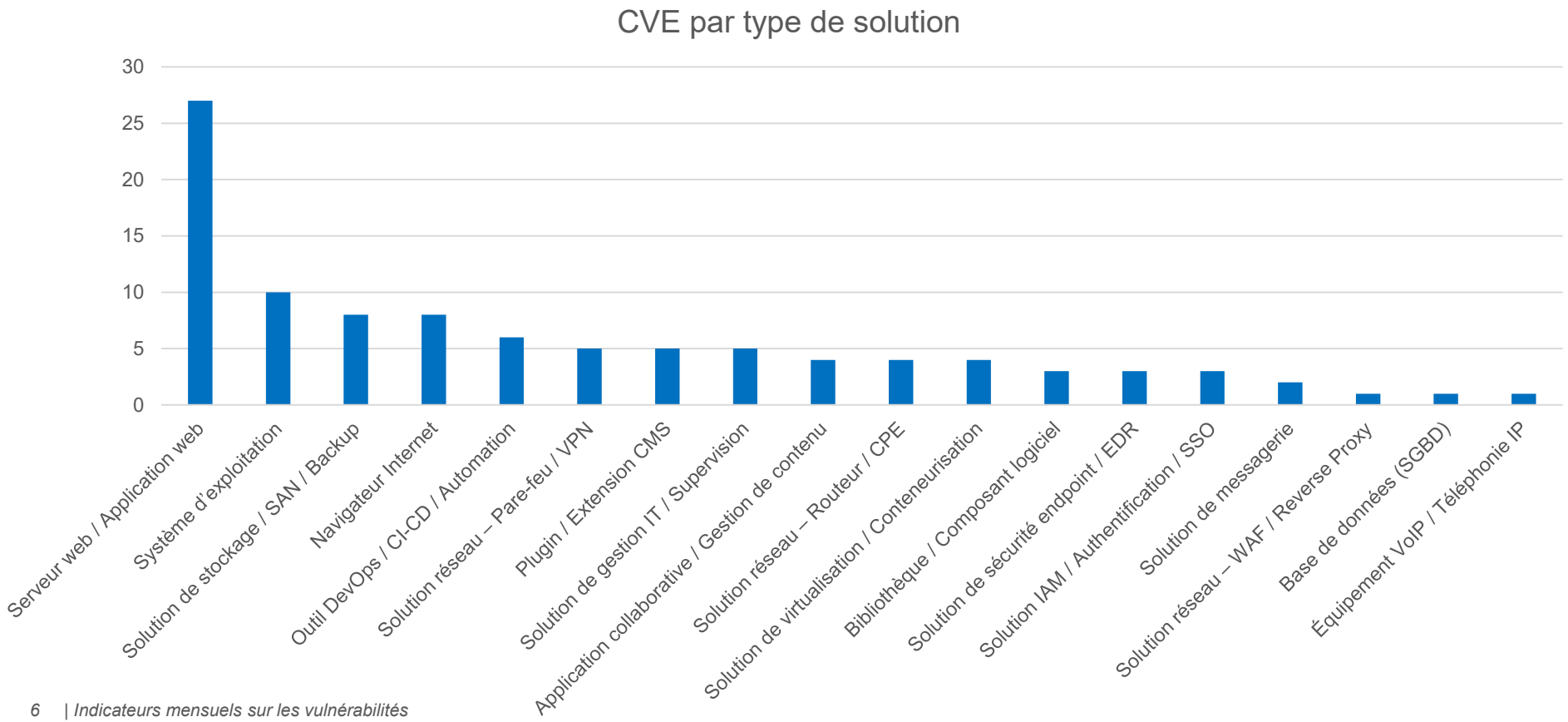
SmarterTools
(CVE-2026-24423)

Exécution de code arbitraire | Exploitée

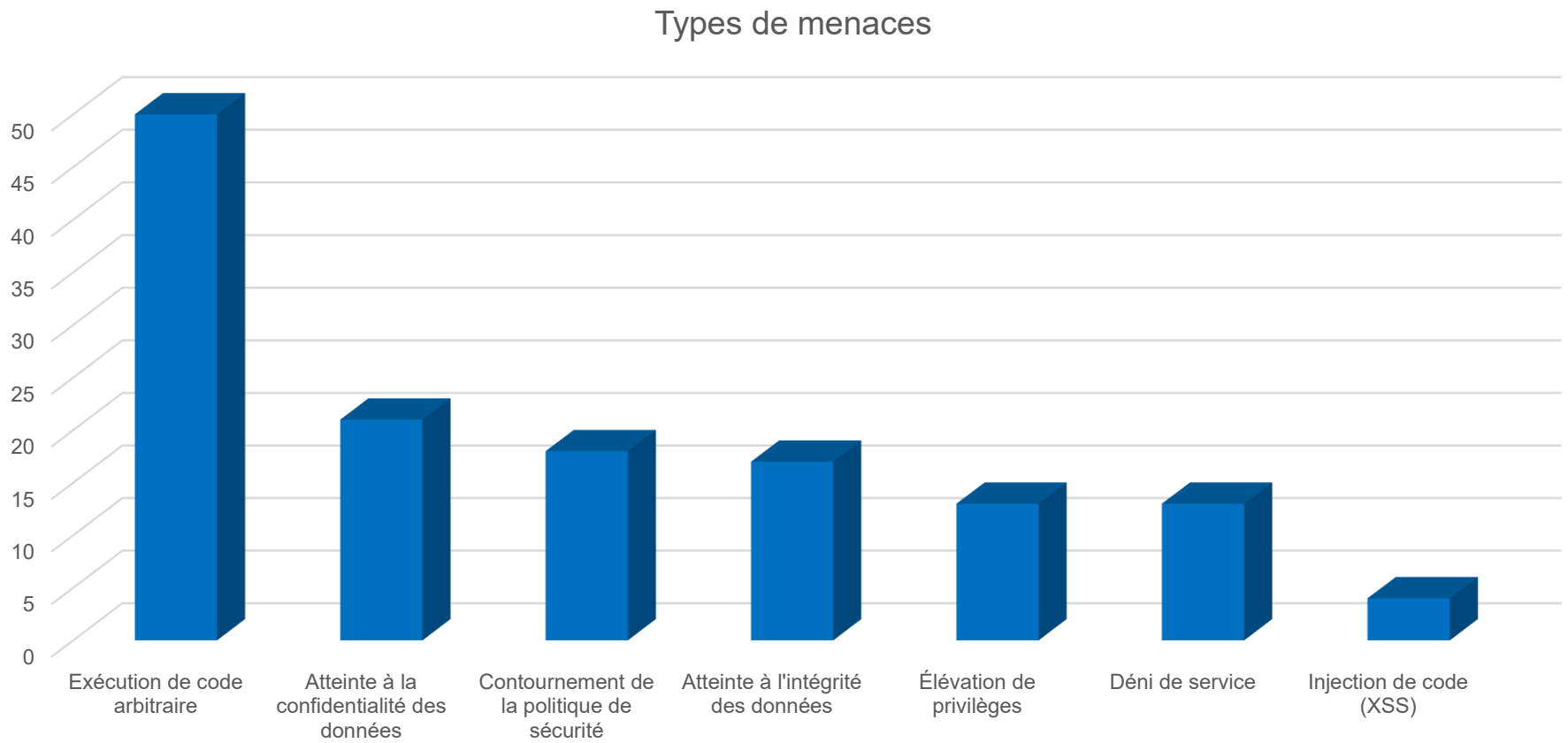
L'exploitation d'une vulnérabilité **d'exécution de code à distance non authentifiée** affecte SmarterMail. Le point d'entrée API ConnectToHub permet à un attaquant distant de **rediriger l'application vers un serveur HTTP** malveillant servant une commande système, laquelle est exécutée par l'application vulnérable.

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 (4 ex-aequo)