CERT Santé

LA E-SANTÉ FRANÇAISE

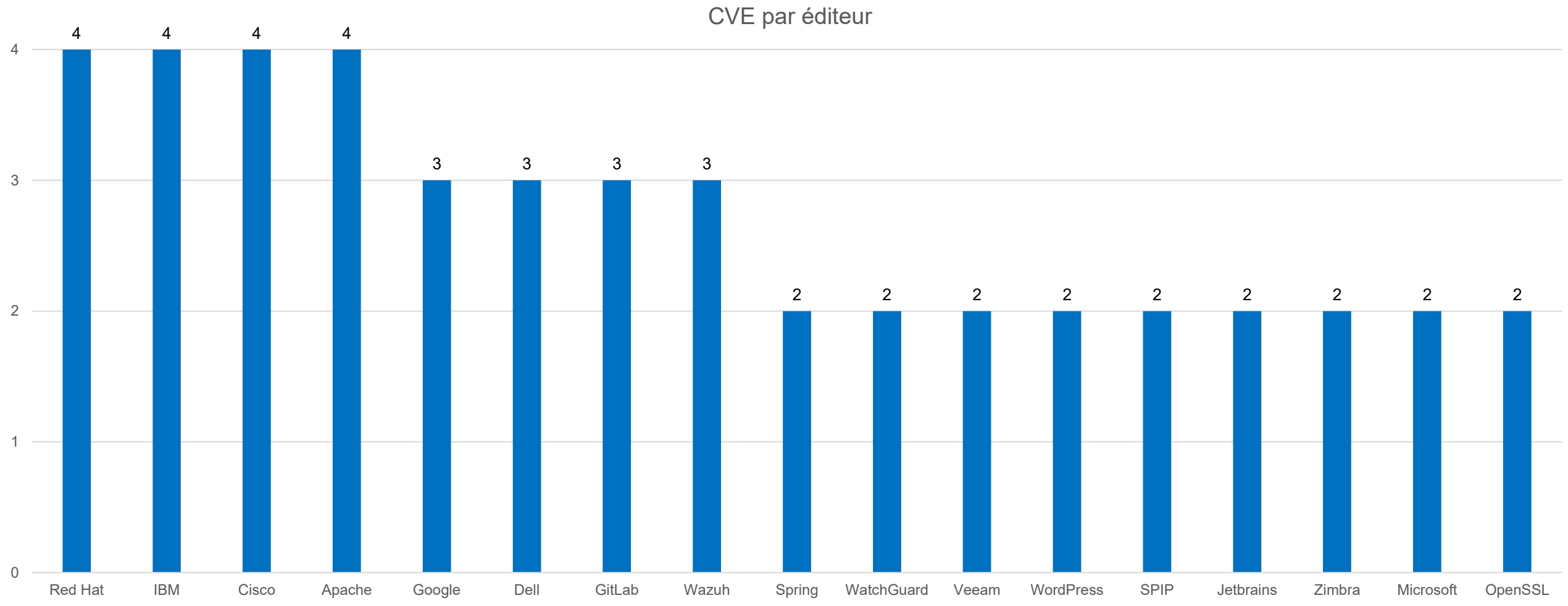
AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

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

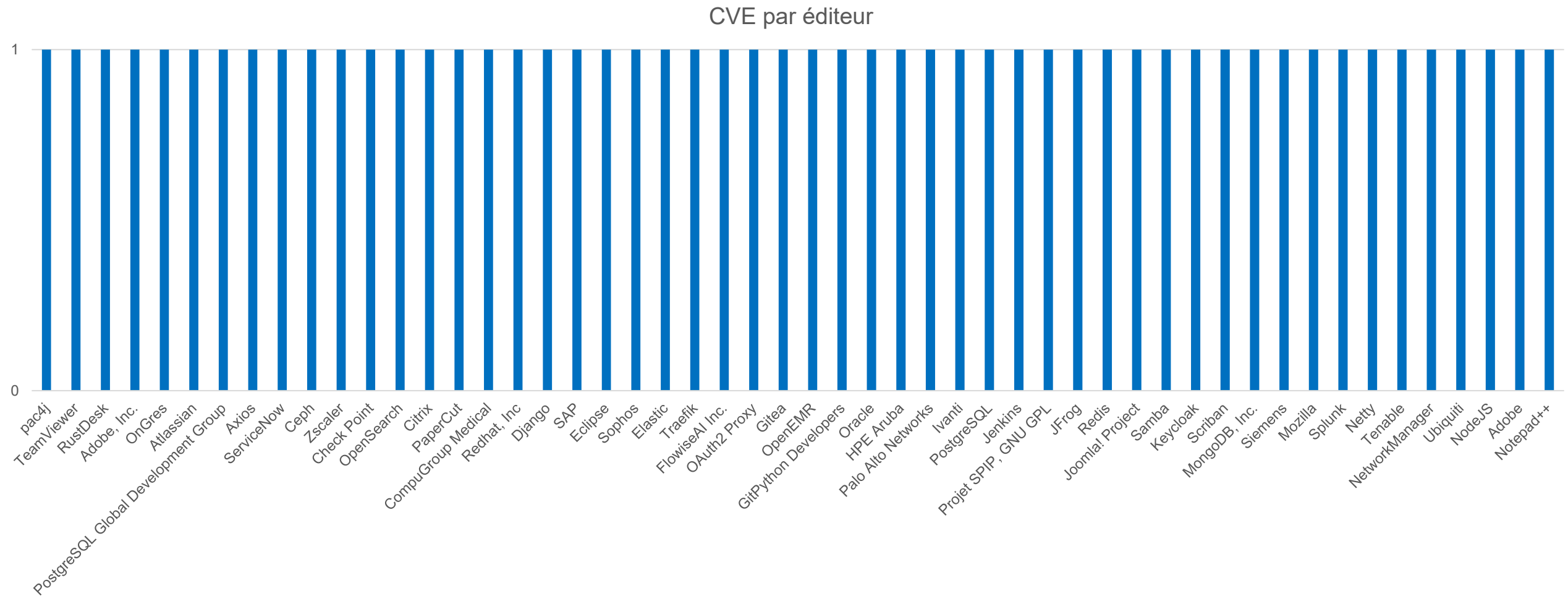
Nombre de CVE par éditeur

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

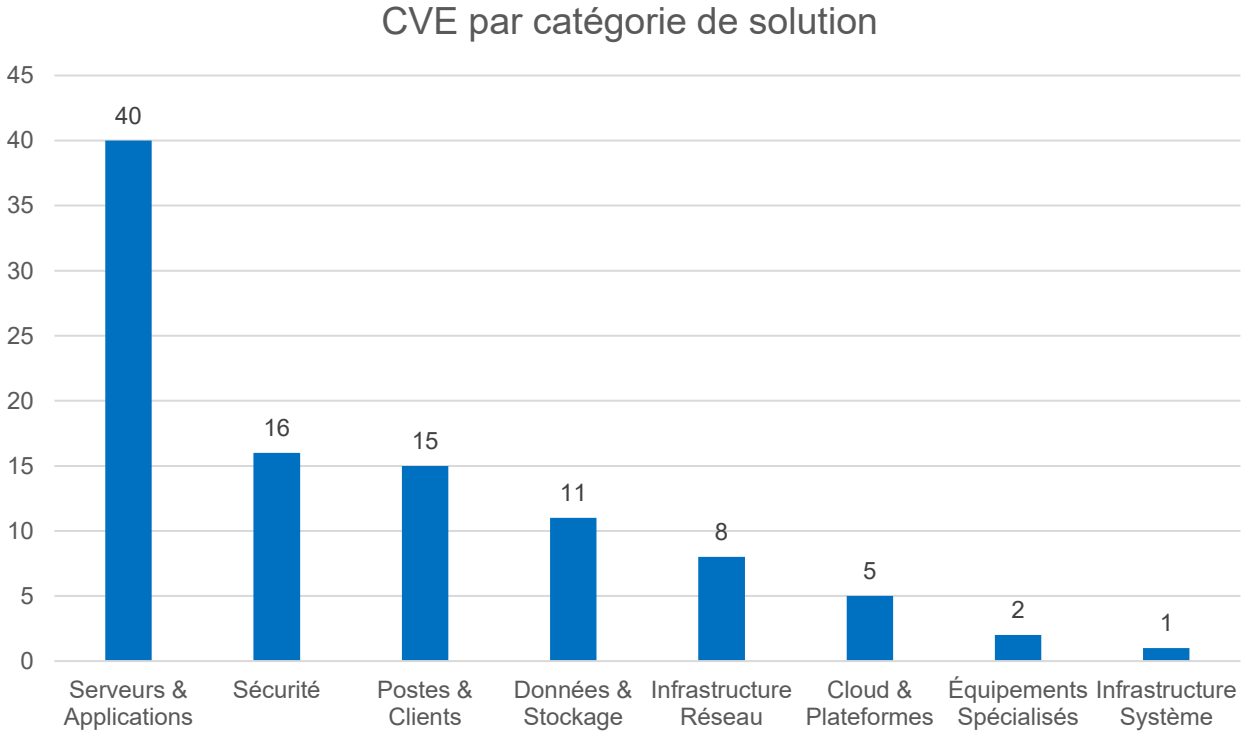


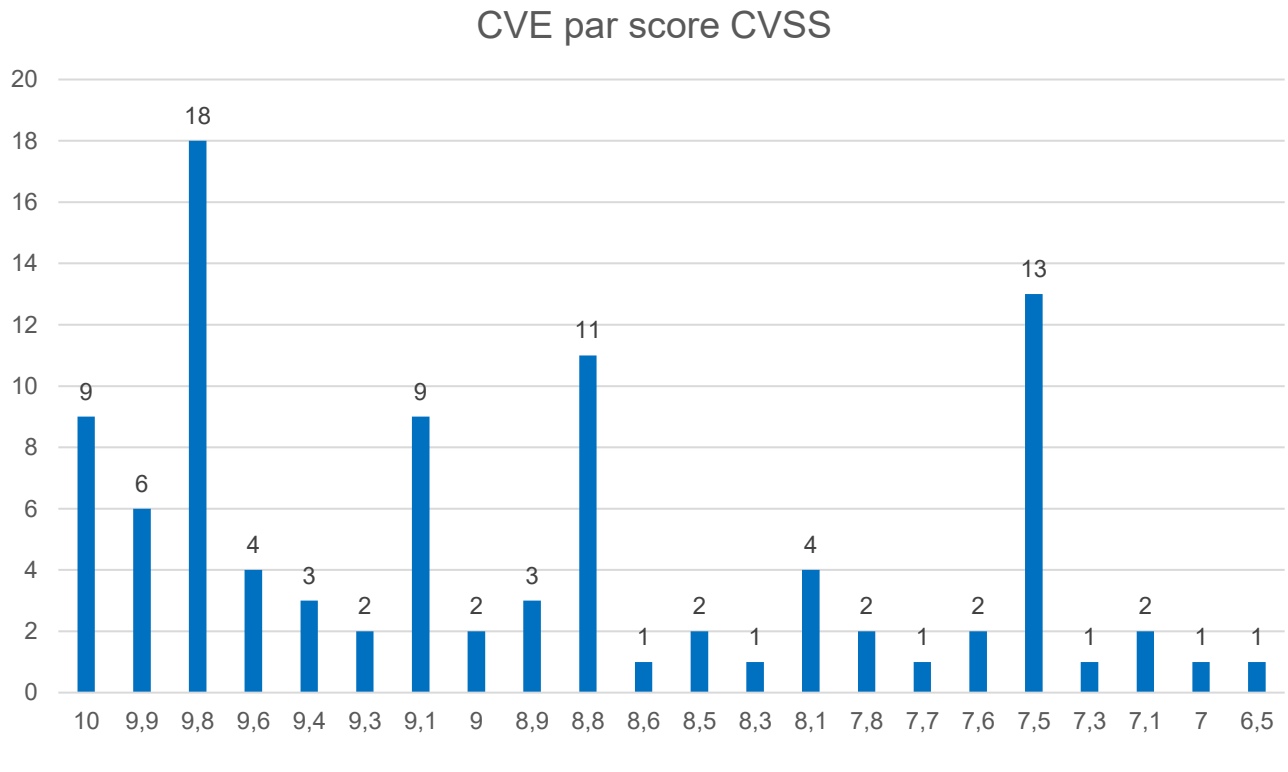
Nombre de CVE par éditeur

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

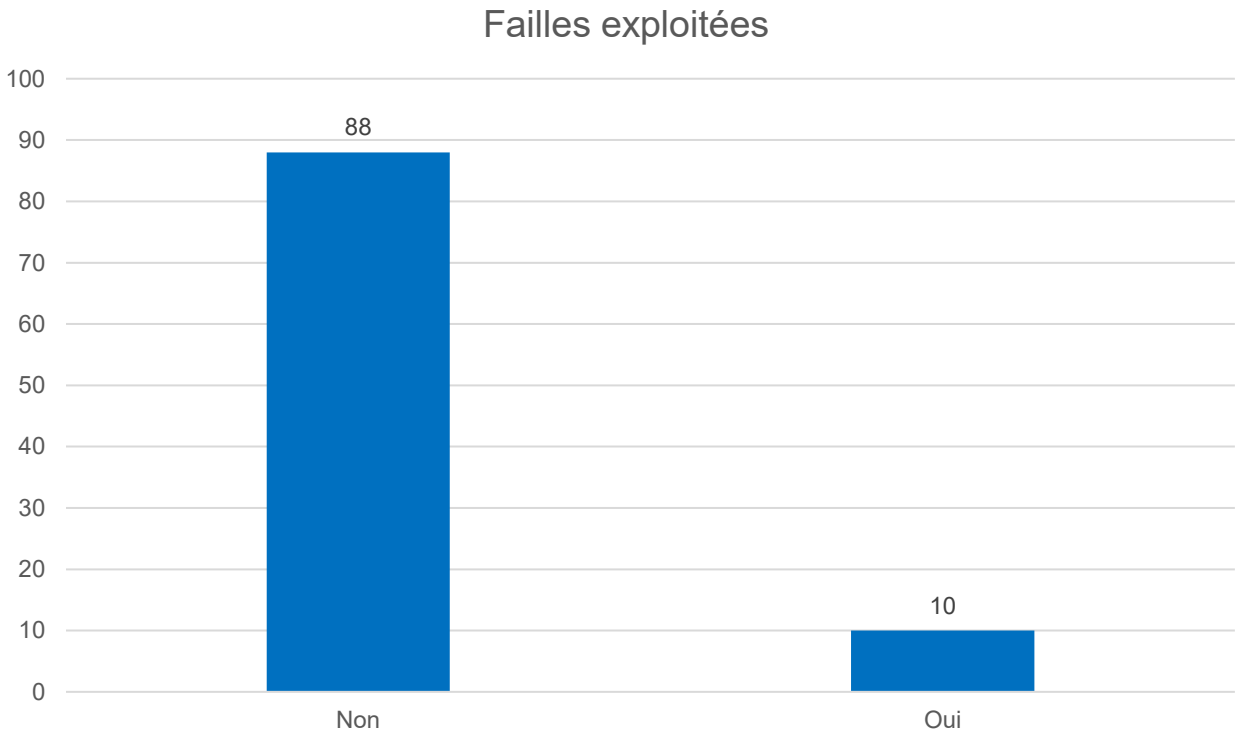


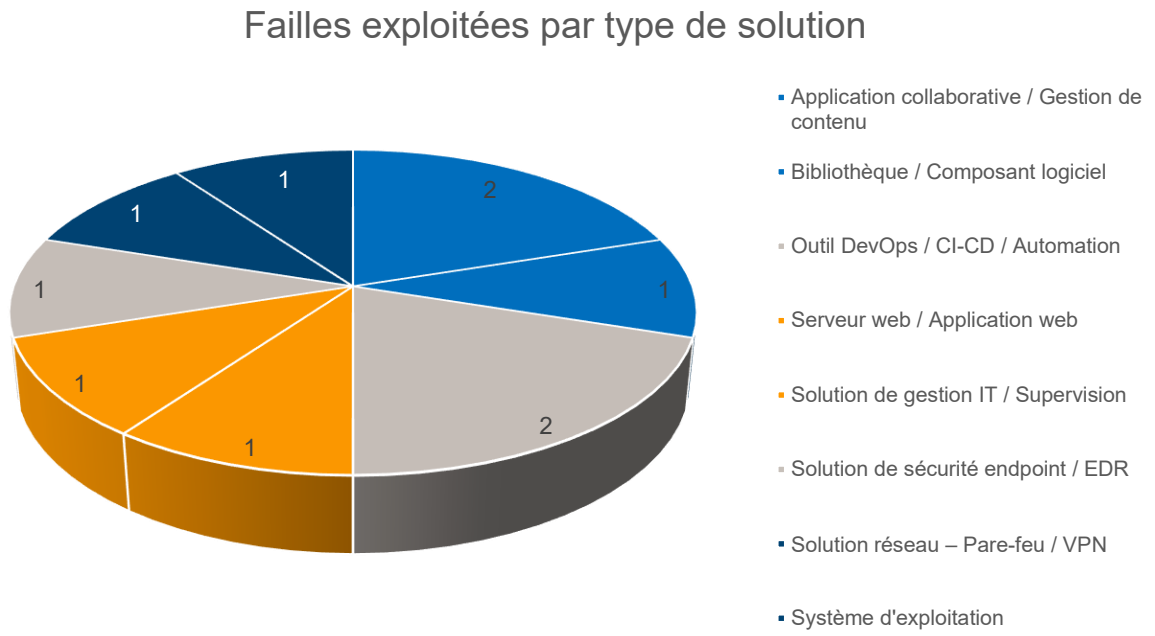
Nombre de CVE par catégorie de produit et score CVSS

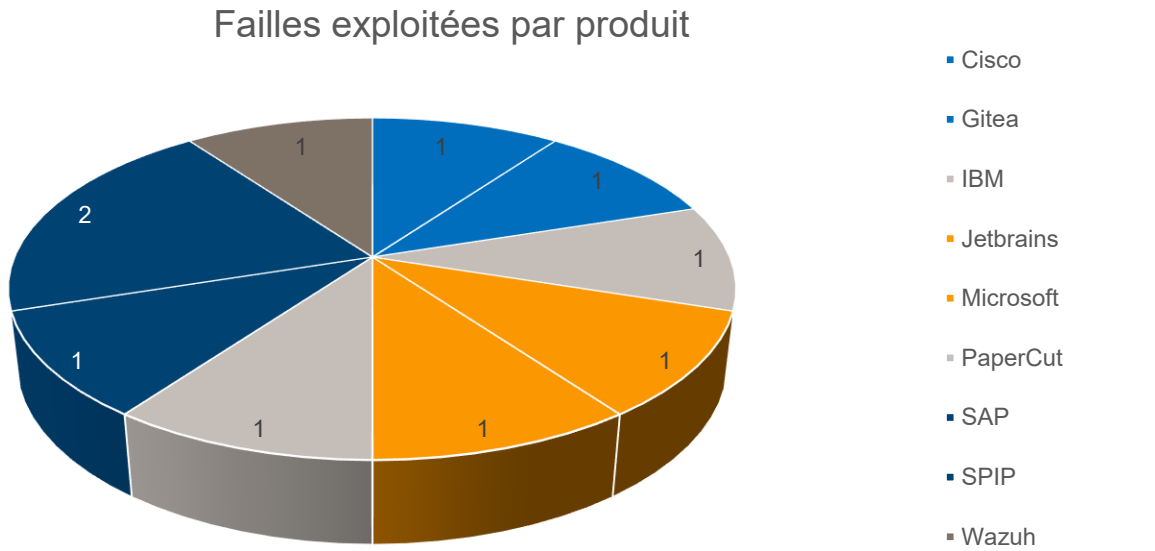




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

9.8 IBM Langflow (CVE-2026-9198)

Exécution de code arbitraire | Exploitée

L'exploitation d'une vulnérabilité d'**injection de code** affectant **IBM Langflow OSS** permet à un attaquant distant non authentifié de chaîner deux points d'entrée insuffisamment sécurisés afin d'obtenir un jeton **SUPERUSER** sans authentification, puis d'exécuter du code arbitraire via la fonction *exec()*, sans interaction utilisateur. Cette faille est inscrite au catalogue **KEV** de la CISA, avec preuve de concept publique disponible. Elle permet une **compromission totale de l'instance Langflow** vulnérable.
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

9.8 Citrix NetScaler ADC/Gateway (CVE-2026-8452)

Exécution de code arbitraire | Exploitée

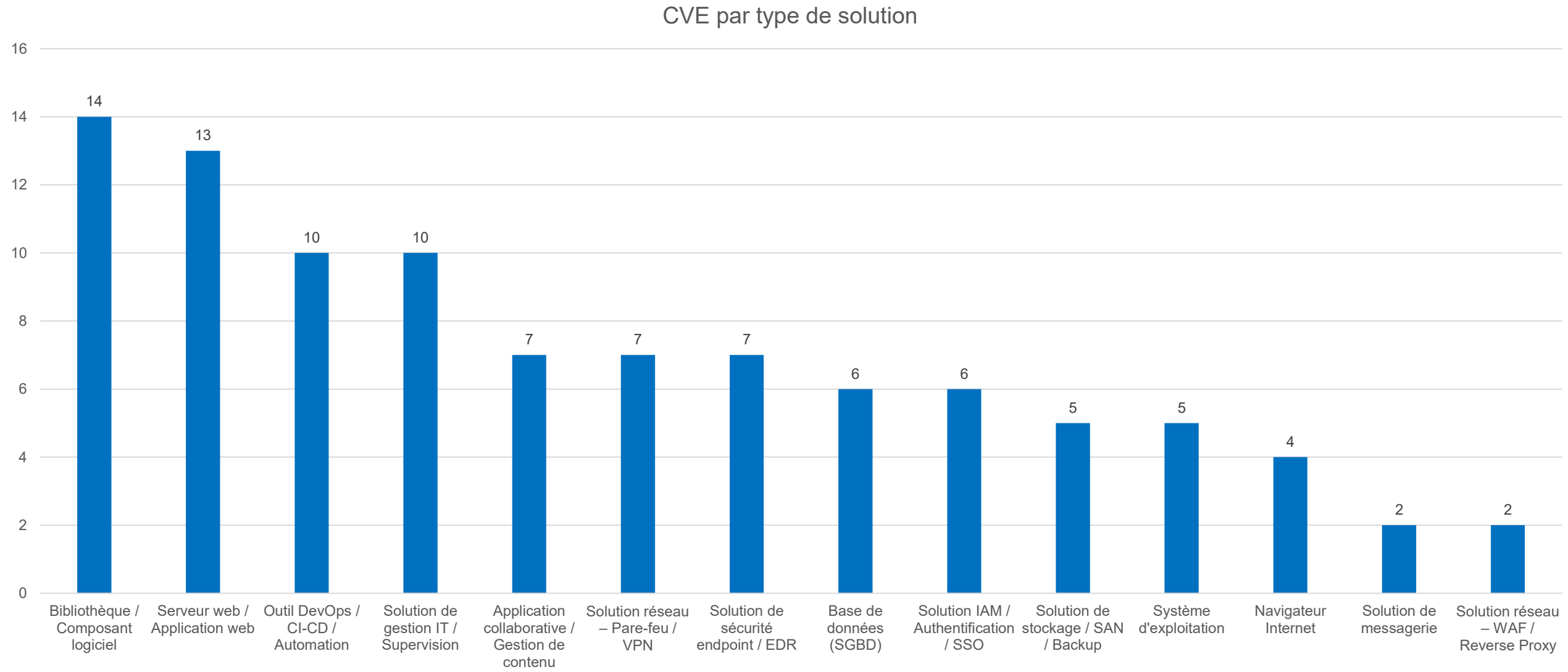
L'exploitation d'une vulnérabilité de **débordement de tampon** (*heap-based buffer overflow*) affectant **NetScaler ADC** et **NetScaler Gateway**, lorsque l'appliance est configurée en passerelle VPN ou serveur virtuel **AAA**, permet à un attaquant distant non authentifié de provoquer un comportement mémoire imprévisible via une requête réseau spécialement forgée. Initialement qualifiée de déni de service par l'éditeur, la faille a été requalifiée en exécution de code par les chercheurs de **watchTowr**, avec dépôt de web shells constaté sur les appliances non corrigées. Elle permet une **prise de contrôle à distance des appliances Citrix exposées**.
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

9.1 PaperCut NG/MF (CVE-2026-82078)

Exécution de code arbitraire | Exploitée

L'exploitation d'une vulnérabilité de **chargement de classe non sécurisé** (*unsafe reflection*) affectant les utilitaires de connexion aux bases de données de **PaperCut MF** et **PaperCut NG**, combinée à la faille **CVE-2026-81578** de contournement d'authentification, permet à un attaquant distant non authentifié de désigner une classe arbitraire du classpath et d'en faire exécuter le bytecode par la JVM du serveur, sans identifiants valides. Plus de 1 000 instances exposées sur Internet ont été recensées par **ShadowServer**, un scénario qui rappelle la campagne du rançongiciel **Cl0p** ayant visé PaperCut en 2023. Elle permet l'**exécution de bytecode Java arbitraire dans le contexte du serveur PaperCut**.
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables



TOP 5 des failles selon le référentiel CWE