CERT Santé

LA E-SANTÉ FRANÇAISE

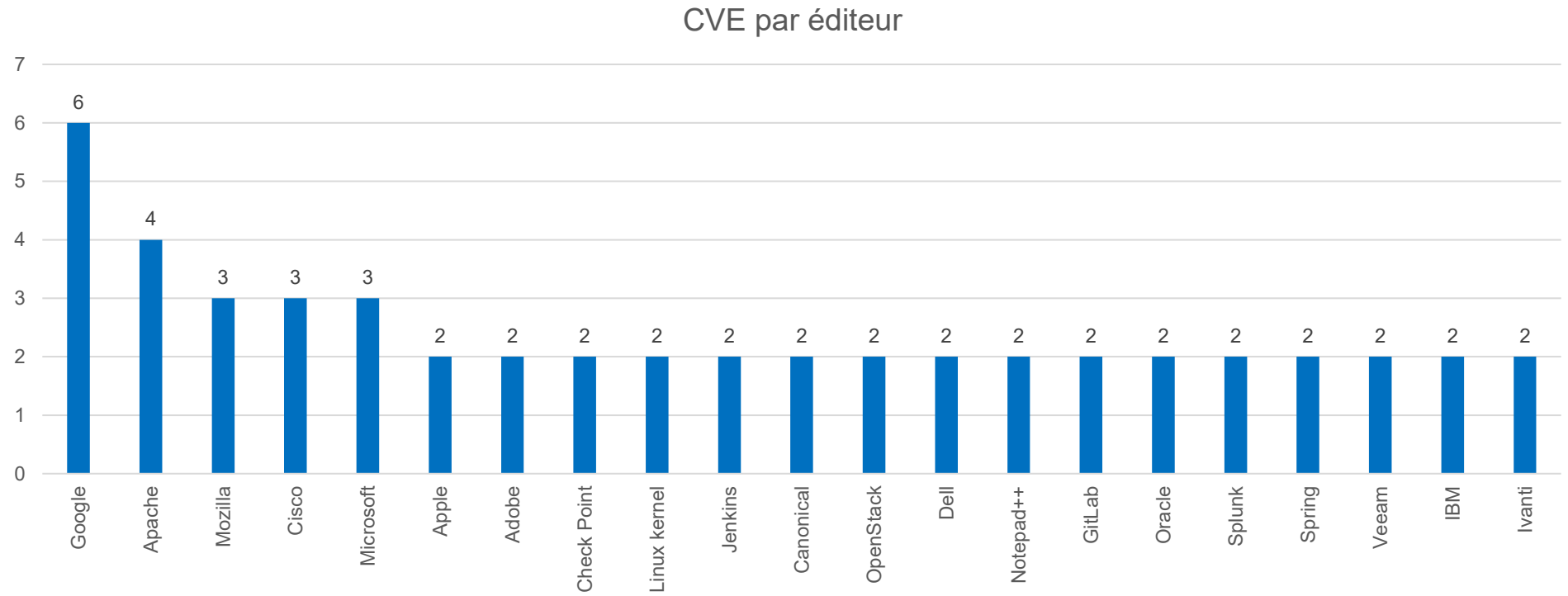
AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

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

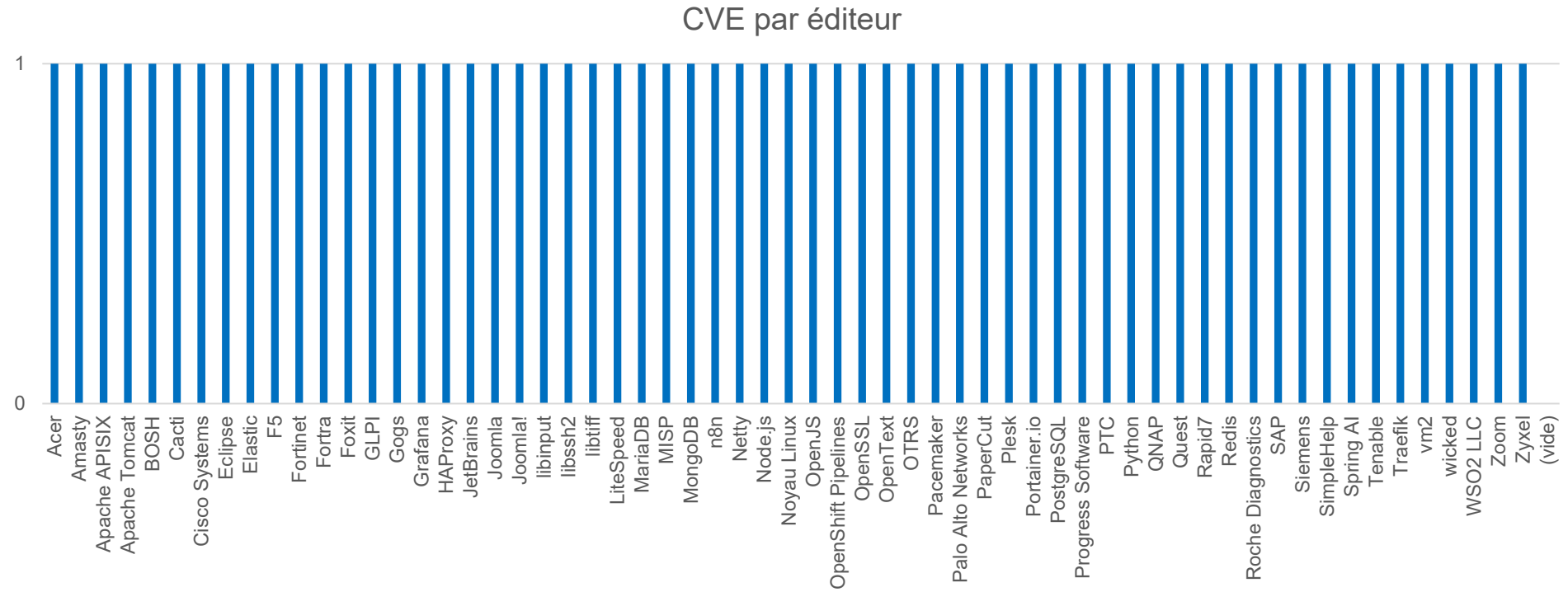
Nombre de CVE par éditeur

112 vulnérabilités ont été analysées et publiées (parmi lesquelles 15 alertes) sur le portail du CERT Santé.

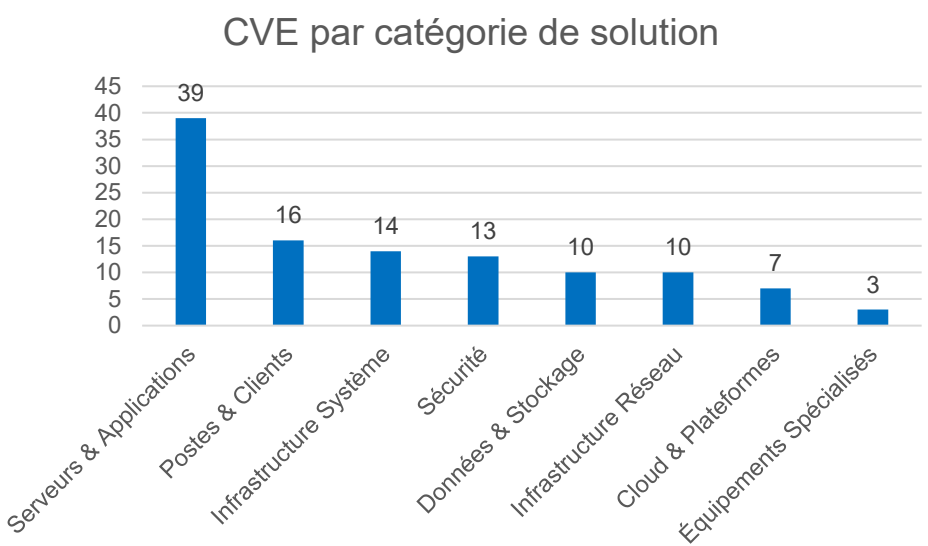


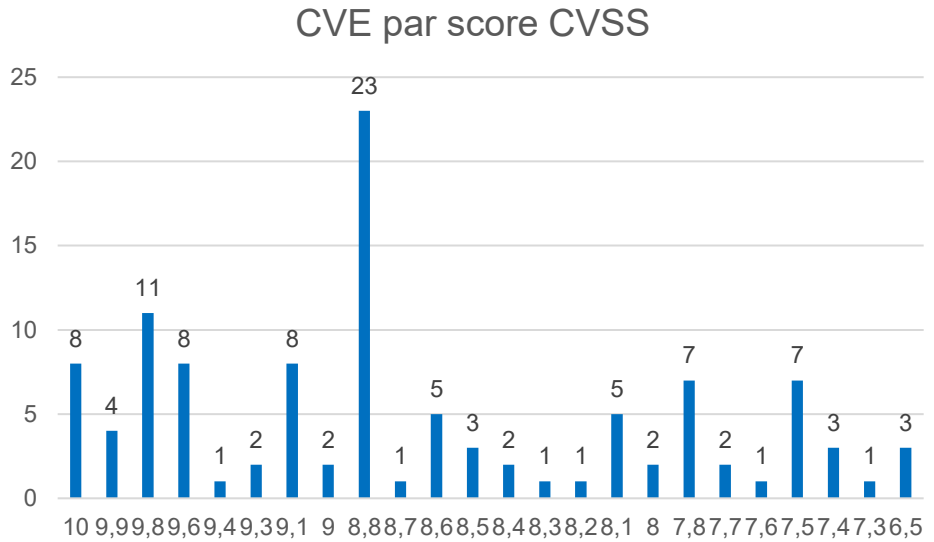
Nombre de CVE par éditeur

112 vulnérabilités ont été analysées et publiées (parmi lesquelles 15 alertes) sur le portail du CERT Santé.

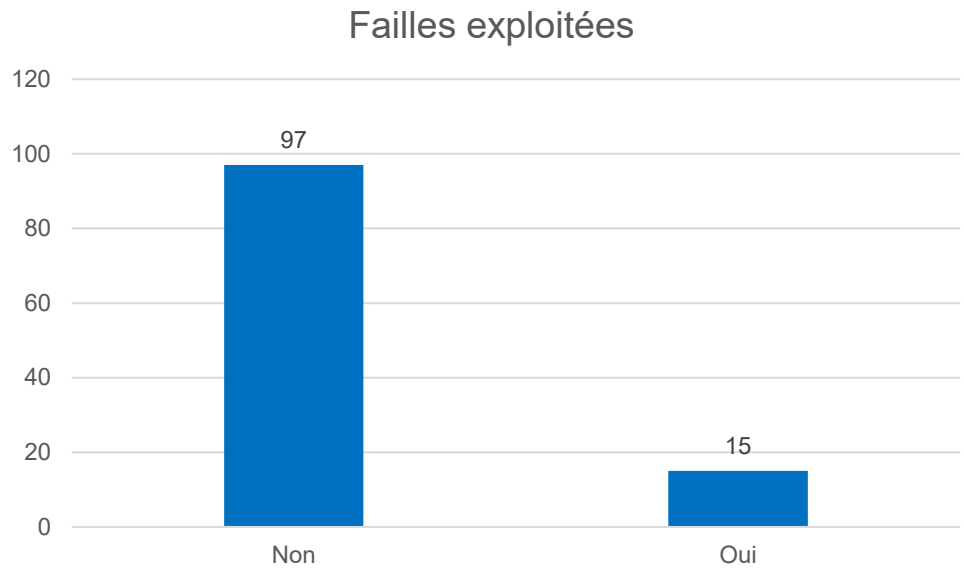


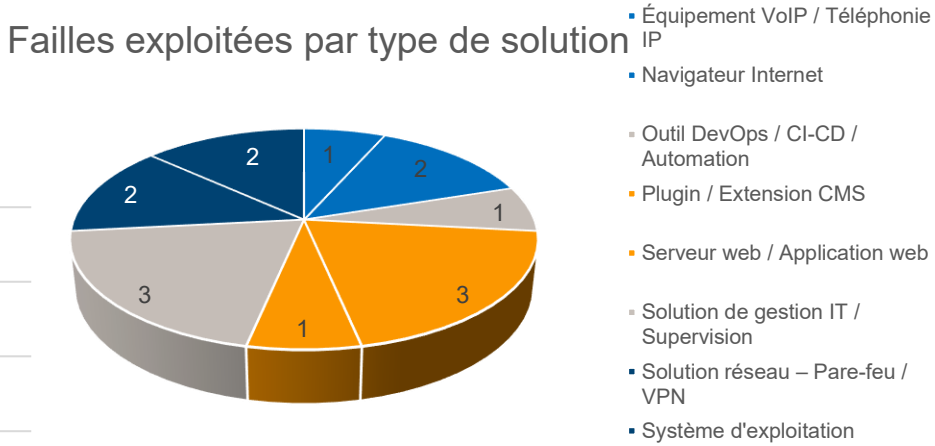
Nombre de CVE par catégorie de produit et score CVSS

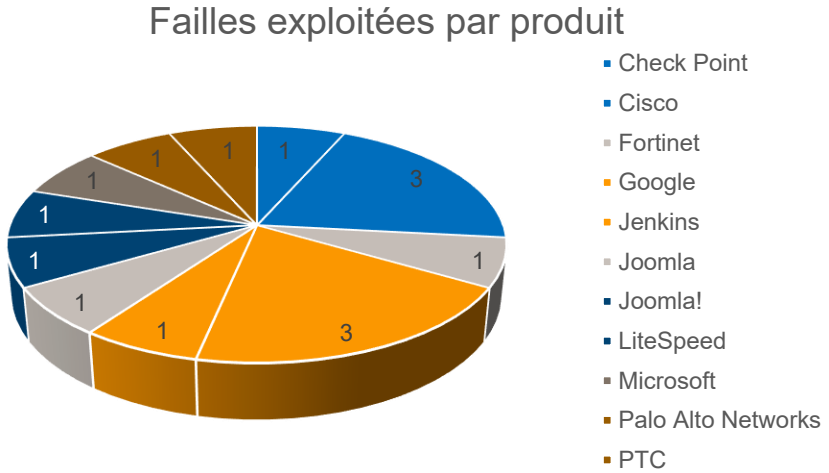




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

9.8

Microsoft Windows Netlogon (CVE-2026-41089)

Exécution de code arbitraire

Exploitée

L'exploitation d'une vulnérabilité de **débordement de tampon** (stack-based buffer overflow) dans le protocole **Netlogon** permet à un attaquant distant non authentifié d'exécuter du code arbitraire avec les **privilèges SYSTEM** sur les **contrôleurs de domaine** via une requête réseau spécialement forgée. Aucune interaction utilisateur n'est requise. Elle permet une **compromission totale de l'Active Directory** et du domaine.

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

9.3

Check Point Security Gateway (CVE-2026-50751)

Contournement de la politique de sécurité

Exploitée

L'exploitation d'une vulnérabilité de **contournement d'authentification** dans le mécanisme **IKEv1** des passerelles VPN Check Point (Remote Access / Mobile Access) permet à un attaquant distant non authentifié d'établir une session VPN sans mot de passe valide, via un défaut de validation de certificat. L'exploitation est attribuée à un affilié du ransomware **Qilin**. Elle permet un **accès non autorisé au réseau interne** de l'organisation cible.

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

9.1

Palo Alto Networks PAN-OS (CVE-2026-0257)

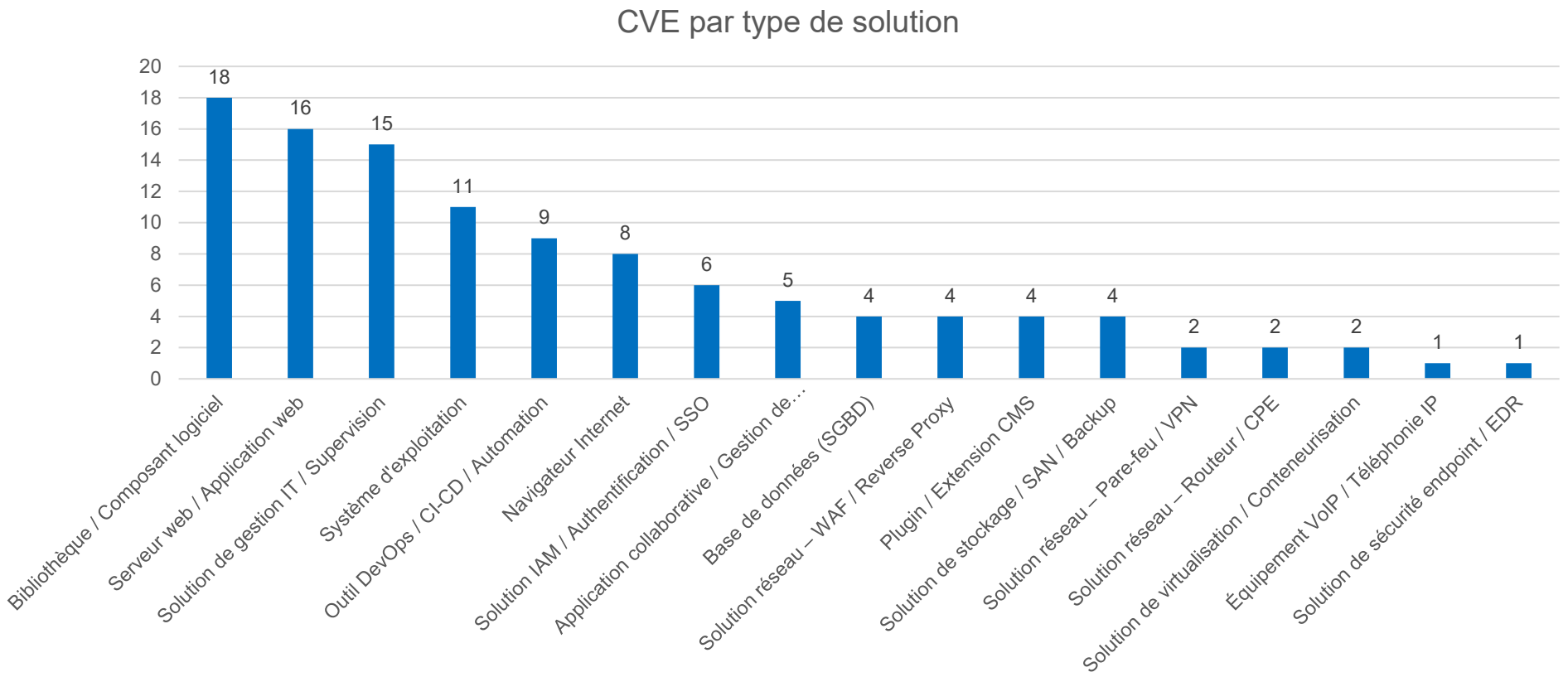
Contournement de la politique de sécurité

Exploitée

L'exploitation d'une vulnérabilité de **contournement d'authentification** dans les composants **portail et passerelle GlobalProtect** permet à un attaquant distant non authentifié de forger et déchiffrer un cookie d'override d'authentification arbitraire, lorsque le certificat de chiffrement des cookies est partagé avec un autre service. Elle permet l'**établissement d'une connexion VPN non autorisée** et l'accès au réseau interne.

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

Types de solutions vulnérables



TOP 5 des failles selon le référentiel CWE