CERT Santé

LA E-SANTÉ FRANÇAISE

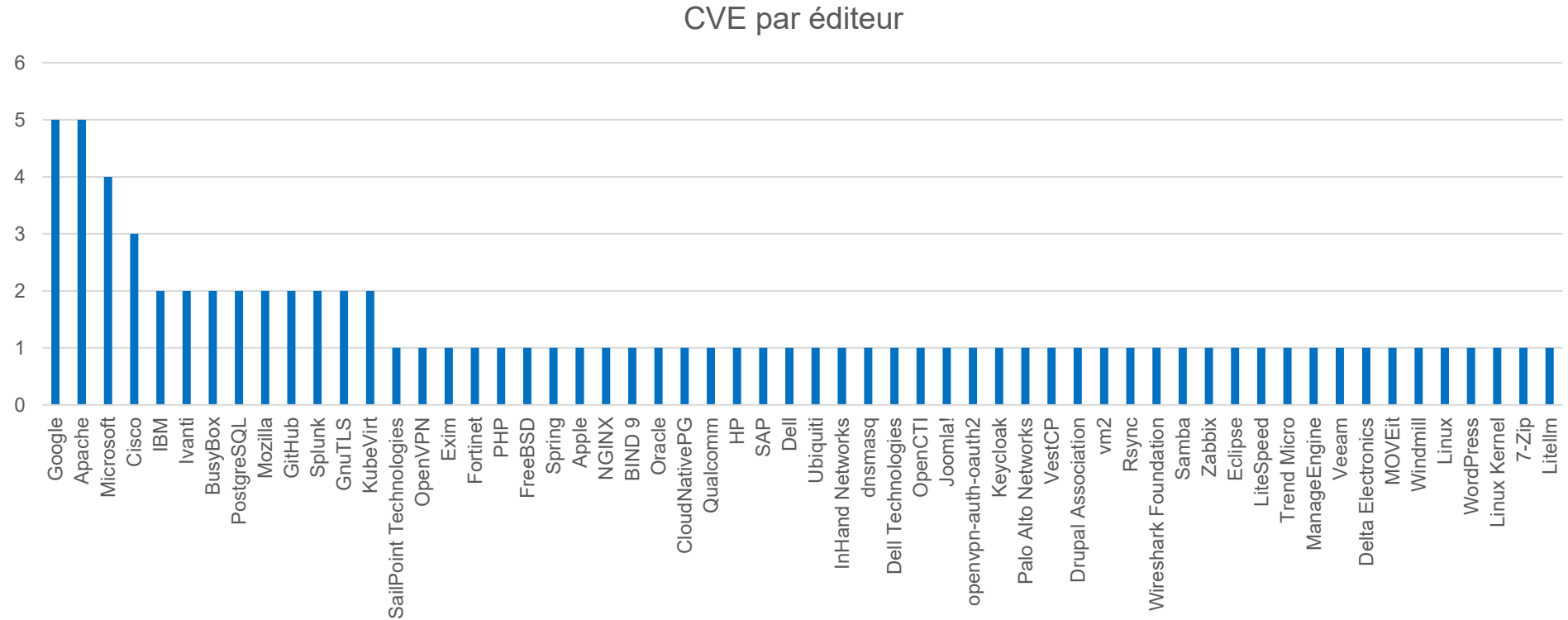
AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

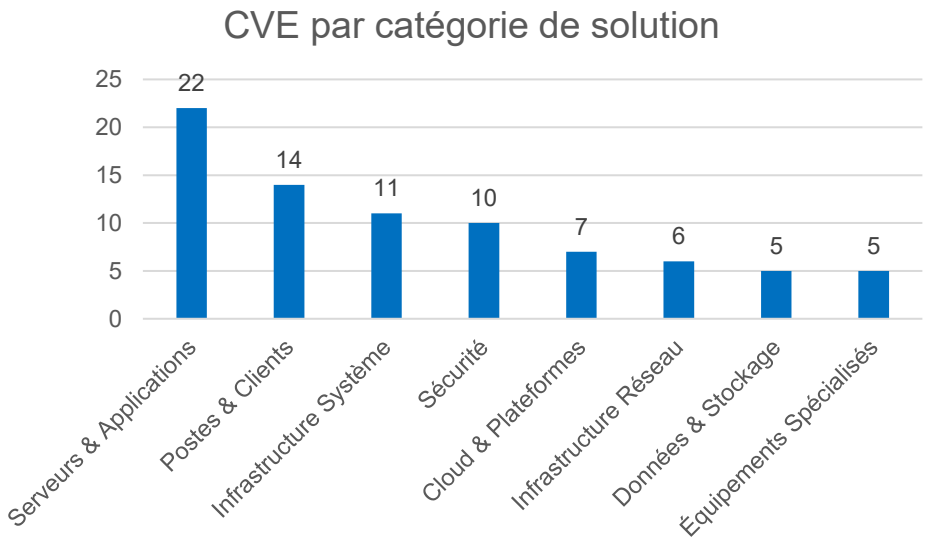
Indicateurs sur la publication des CVE pour le mois de mai 2026

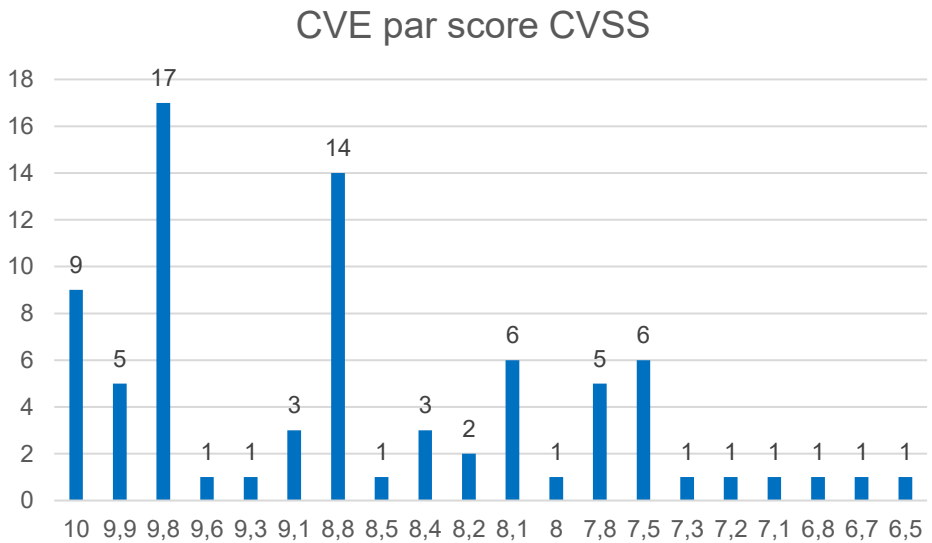
Nombre de CVE par éditeur

80 vulnérabilités ont été analysées et publiées (parmi lesquelles 12 alertes) sur le portail du CERT Santé.

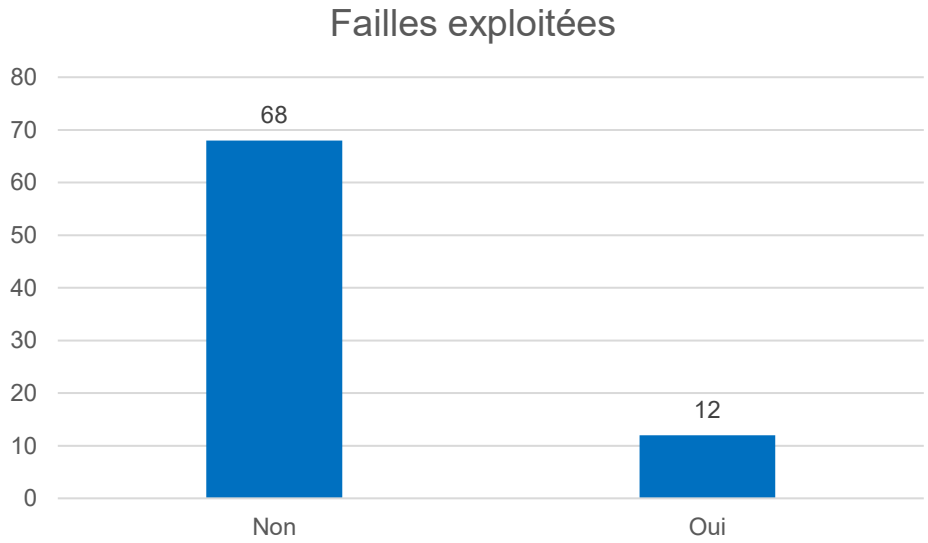


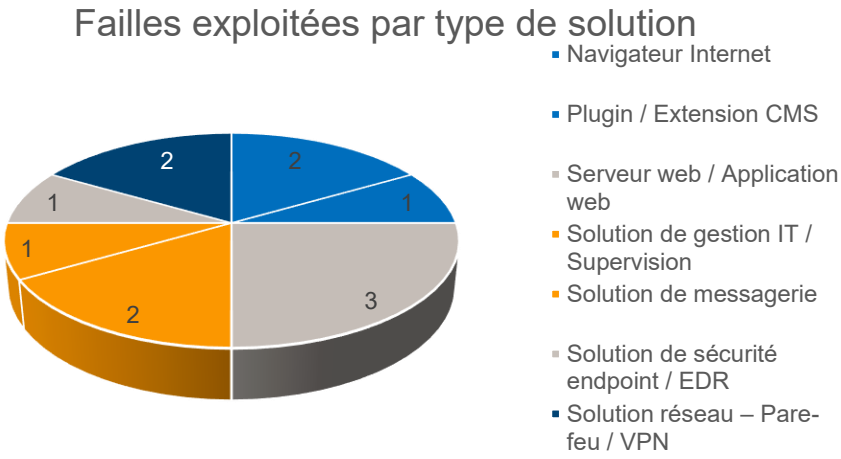
Nombre de CVE par catégorie de produit et score CVSS

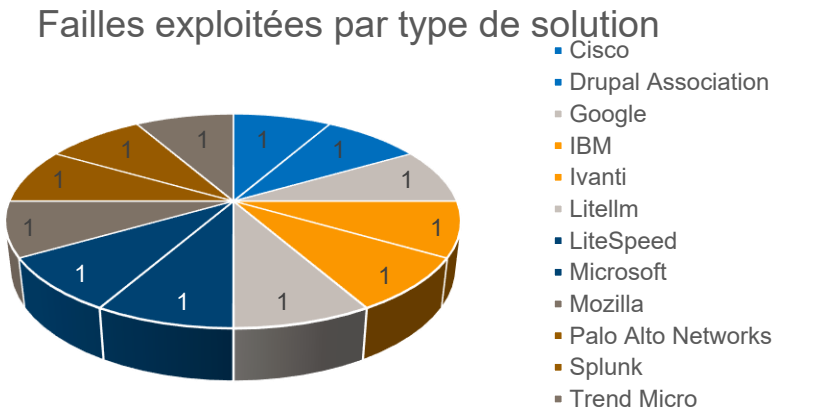




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

10

Cisco Catalyst SD-WAN
(CVE-2026-20182)

Contournement de la politique de sécurité

Exploitée

L'exploitation d'une vulnérabilité de **contournement d'authentification** dans le mécanisme de peering du service **vdaemon** de **Cisco Catalyst SD-WAN Controller** permet à un attaquant distant non authentifié d'obtenir les **privilèges administrateurs** sur le plan de contrôle SD-WAN via une requête DTLS forgée sur le port UDP 12346. L'exploitation est attribuée à l'acteur étatique UAT-8616. Elle permet une **compromission totale du fabric réseau SD-WAN**.

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

9.8

Palo Alto Networks PAN-OS
(CVE-2026-0300)

Exécution de code arbitraire

Exploitée

L'exploitation d'une vulnérabilité de type **débordement de tampon** dans le **portail d'authentification User-ID (Captive Portal)** de **PAN-OS** permet à un attaquant distant non authentifié d'exécuter du code arbitraire avec les **privilèges root** sur les pare-feux PA-Series et VM-Series. Aucune interaction utilisateur n'est requise. Elle permet une **compromission complète du pare-feu périmétrique**.

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

9.8

LiteLLM Proxy (BerriAI)
(CVE-2026-42208)

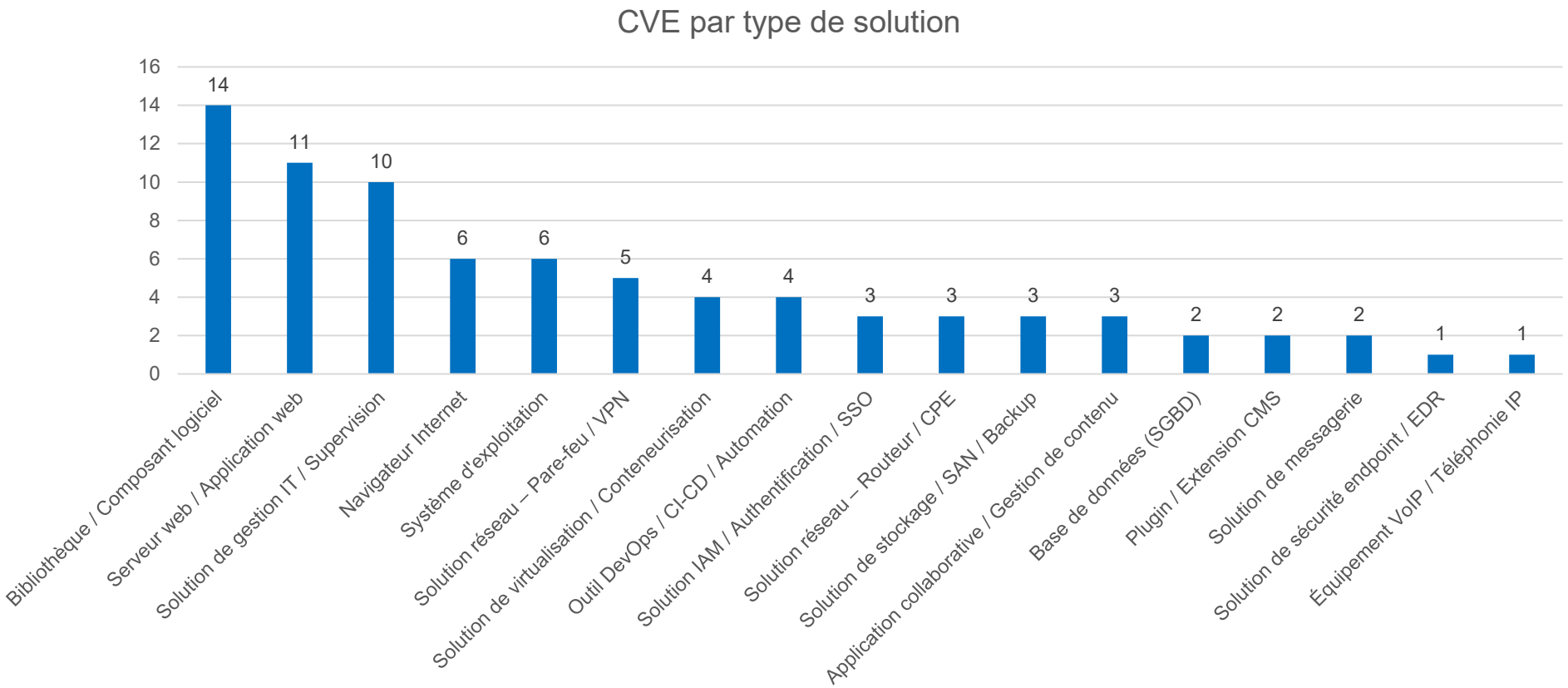
Atteinte à la confidentialité des données

Exploitée

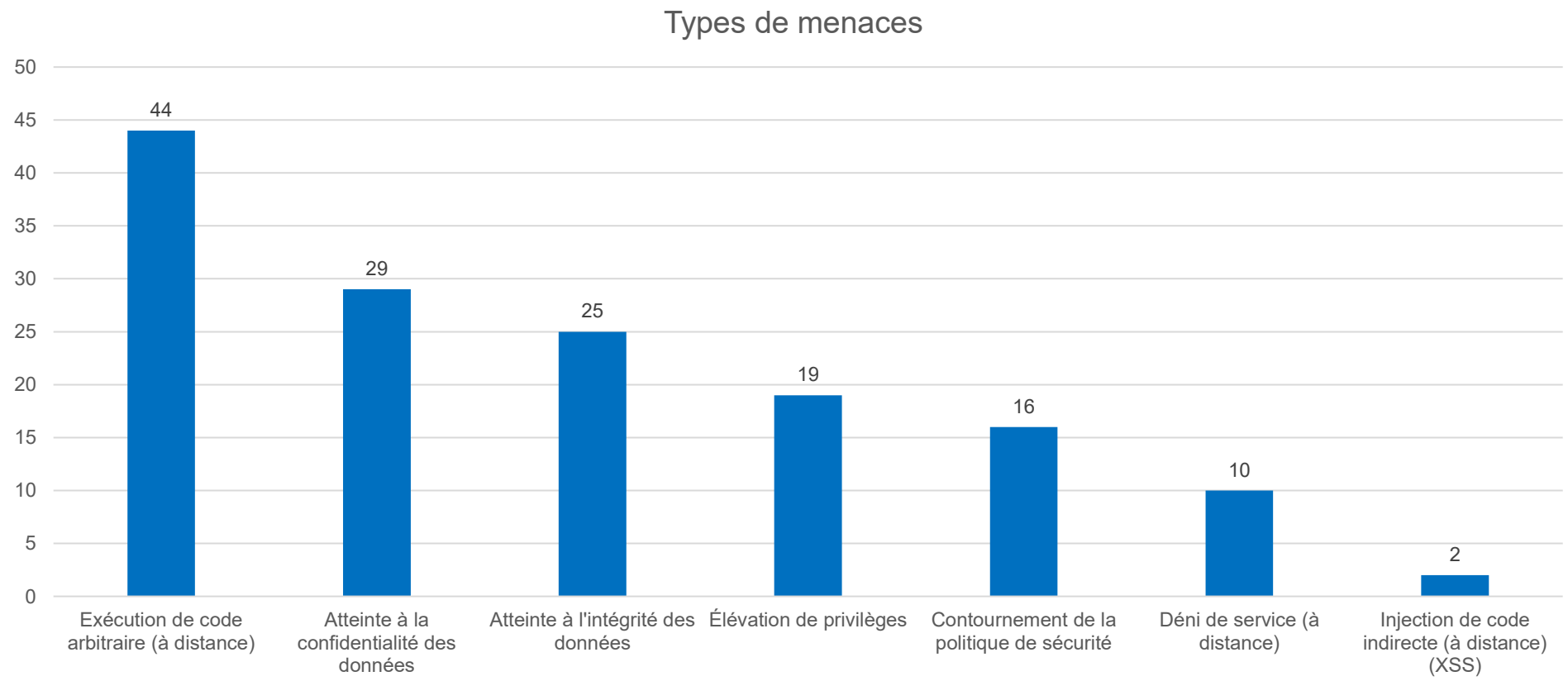
L'exploitation d'une vulnérabilité d'**injection SQL pré-authentification** dans le chemin de vérification de clé API du proxy **LiteLLM** permet à un attaquant distant non authentifié d'interagir directement avec la base **PostgreSQL** via un en-tête **Authorization: Bearer** forgé. Elle permet l'**exfiltration de l'ensemble des credentials et clés API** des fournisseurs IA configurés.

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)