CERT Santé

LA E-SANTÉ FRANÇAISE

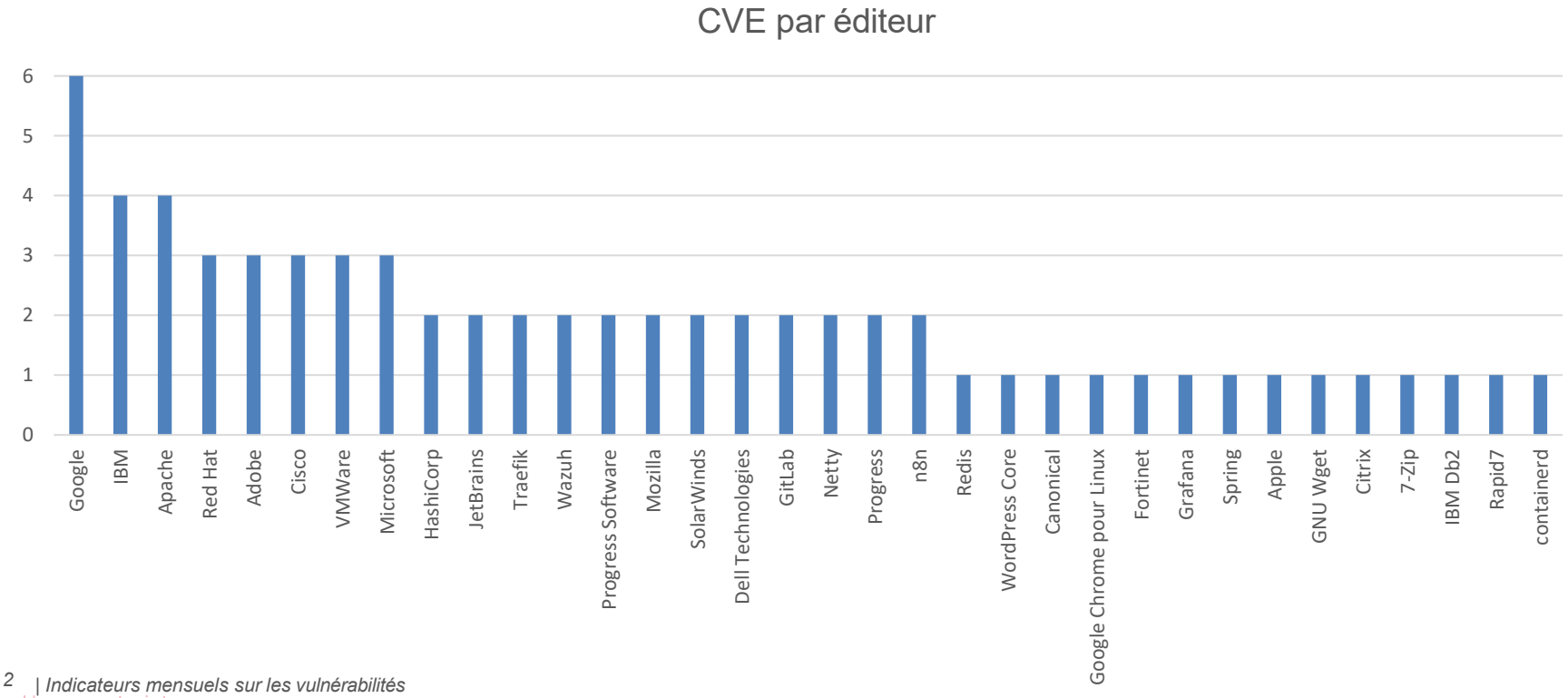
AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

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

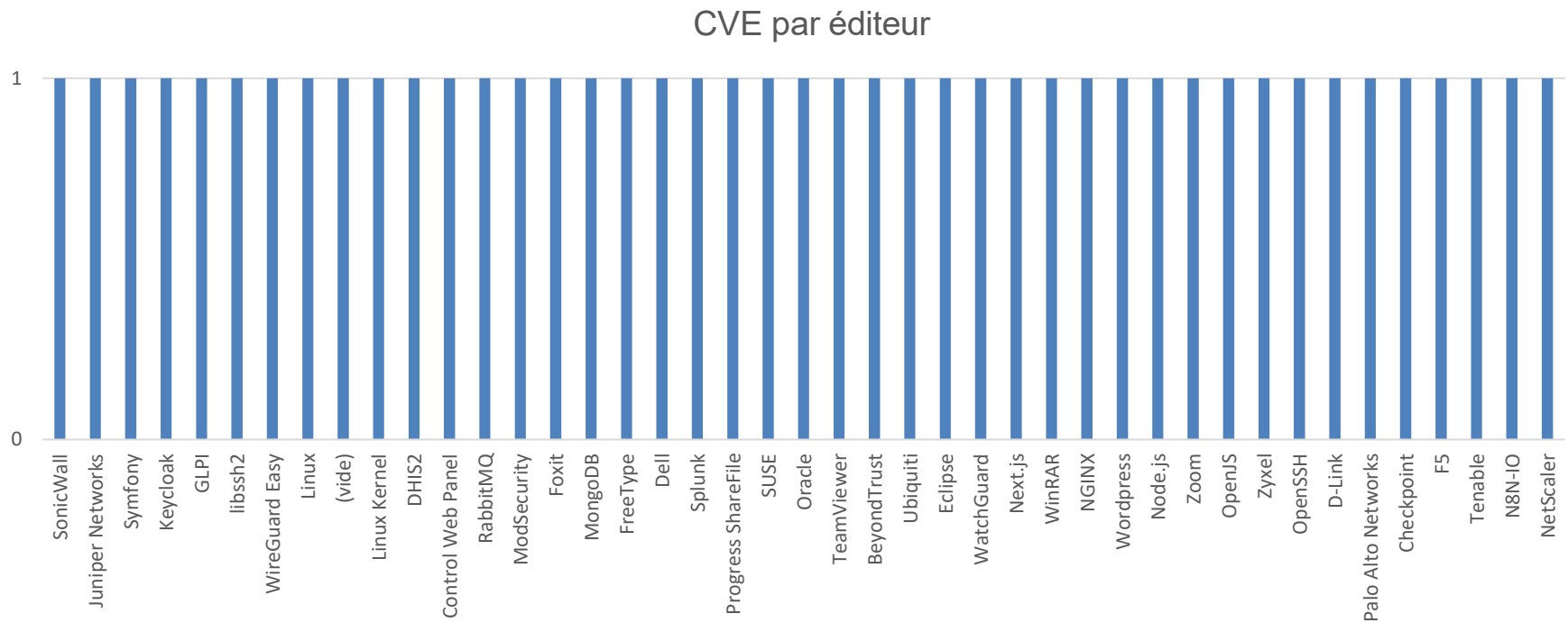
Nombre de CVE par éditeur

110 vulnérabilités ont été analysées et publiées (parmi lesquelles 6 alertes) sur le portail du CERT Santé.

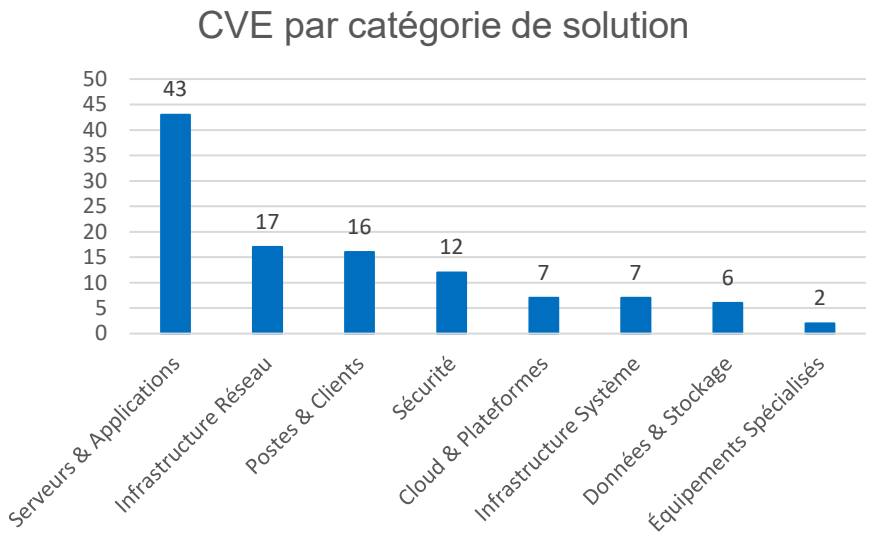


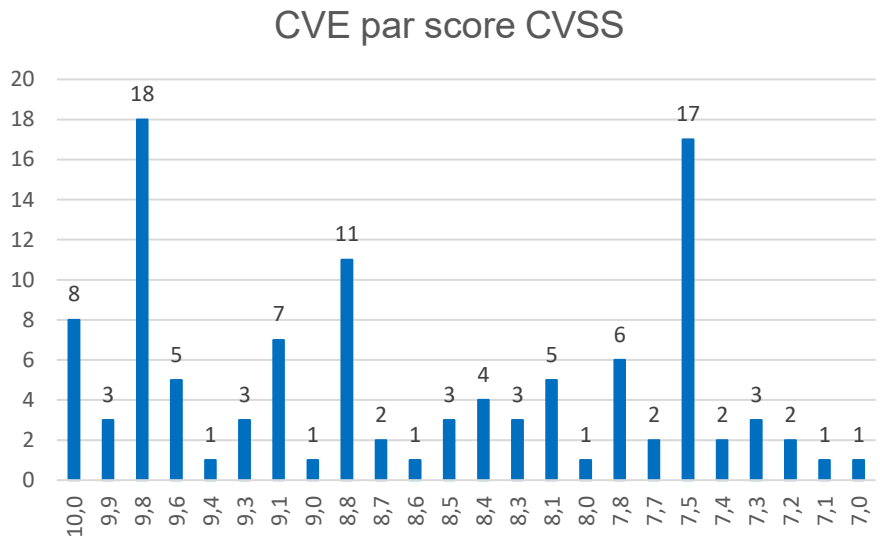
Nombre de CVE par éditeur

110 vulnérabilités ont été analysées et publiées (parmi lesquelles 6 alertes) sur le portail du CERT Santé.

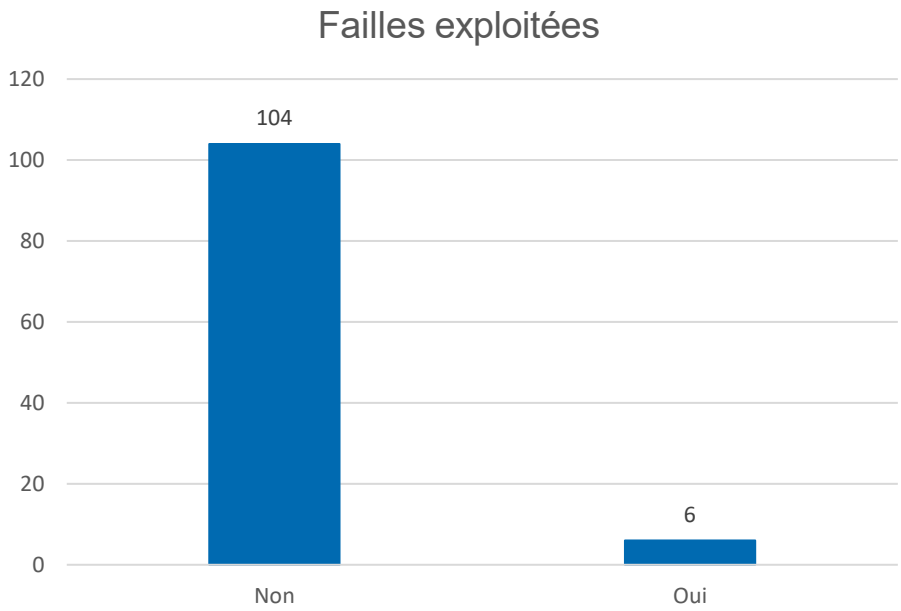


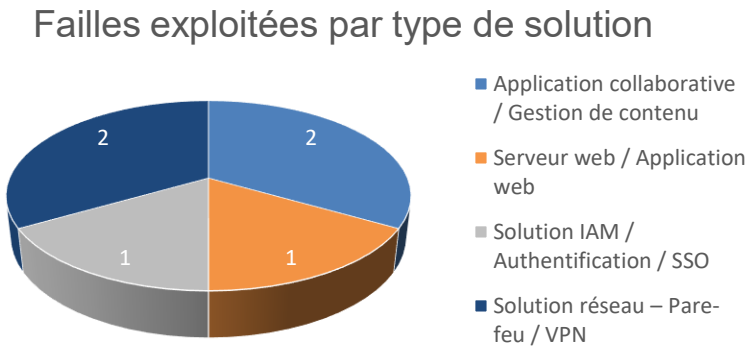
Nombre de CVE par catégorie de produit et score CVSS

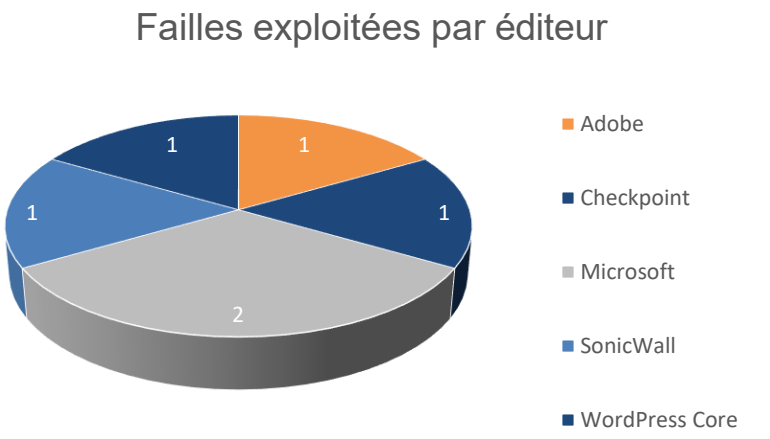




Vulnérabilités exploitées







Les vulnérabilités critiques à surveiller

Microsoft SharePoint Server

9.8

([CVE-2026-56164](#))

Contournement de la politique de sécurité

Exploitée

L'exploitation d'une vulnérabilité de **contrôle d'accès insuffisant** dans Microsoft Office SharePoint permet à un **attaquant distant non authentifié** d'exécuter une fonction critique du serveur via une requête réseau spécialement forgée, sans privilège préalable ni interaction utilisateur. Elle permet une **élévation de privilèges à distance** et peut conduire à une **compromission complète du serveur SharePoint.**

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

WordPress (WP2Shell)

9.8

([CVE-2026-63030](#))

Exécution de code arbitraire (à distance)

Exploitée

L'exploitation d'une vulnérabilité de **confusion de routage** (Route Confusion) dans l'API REST de WordPress permet à un **attaquant distant non authentifié** de contourner les mécanismes de validation des requêtes via des requêtes spécialement forgées. Combinée à la vulnérabilité d'injection SQL CVE-2026-60137, elle peut conduire à une **exécution de code arbitraire à distance (RCE)**. Elle peut entraîner une **compromission complète du site WordPress**, la prise de contrôle du serveur sous-jacent et l'accès à l'ensemble des données hébergées.

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

Check Point SmartConsole

9.1

([CVE-2026-16232](#))

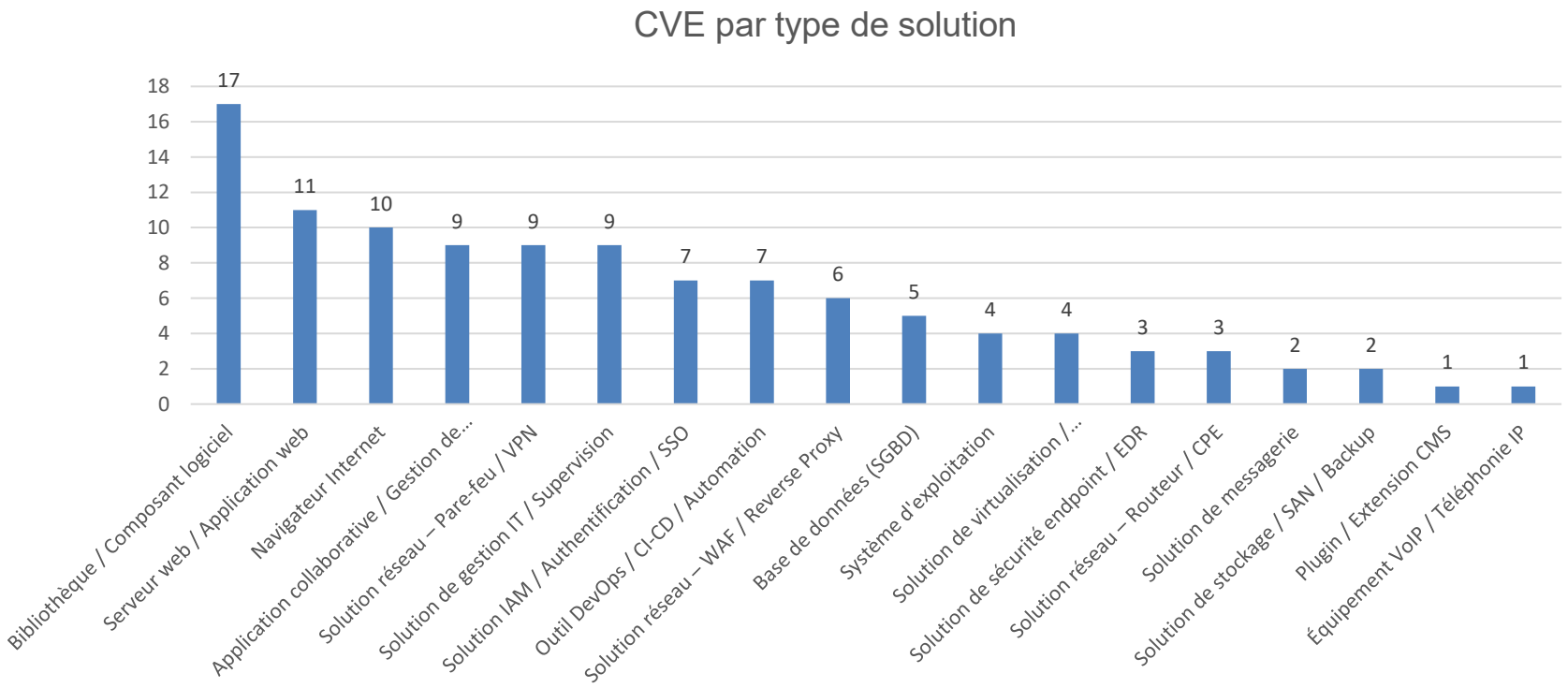
Contournement d'authentification

Exploitée

L'exploitation d'une vulnérabilité de **contournement d'authentification** (Authentication Bypass) dans le processus de connexion SmartConsole de Check Point permet à un **attaquant distant non authentifié** d'obtenir un jeton d'authentification valide et d'accéder à l'interface d'administration avec des privilèges complets. Cette attaque peut être réalisée sans privilège préalable ni interaction utilisateur lorsque le serveur de management est accessible et insuffisamment restreint. Elle permet une **prise de contrôle complète du serveur de gestion**, pouvant conduire à la modification des politiques de sécurité, des configurations réseau, des règles de filtrage et de l'ensemble des équipements administrés par la plateforme.

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

Types de solutions vulnérables



TOP 5 des failles selon le référentiel CWE