CERT Santé

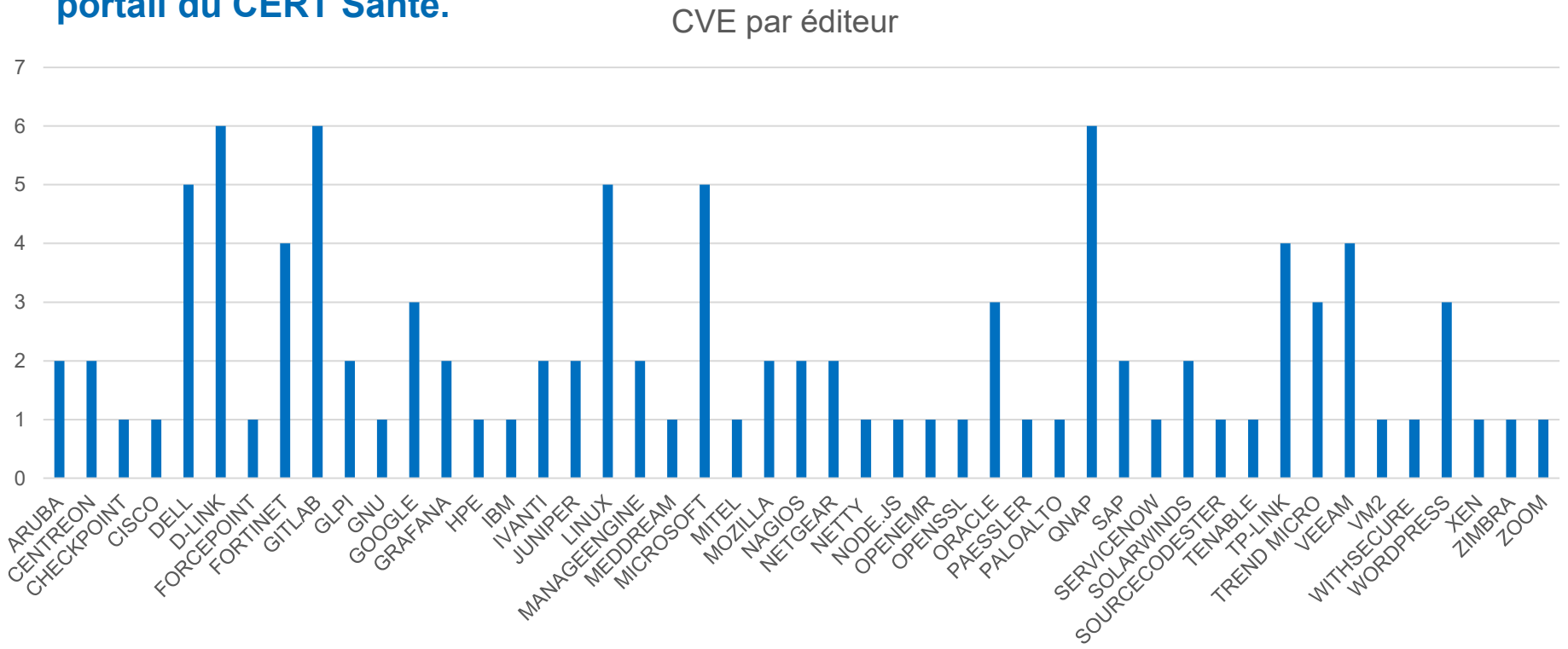
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

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

Février 2026

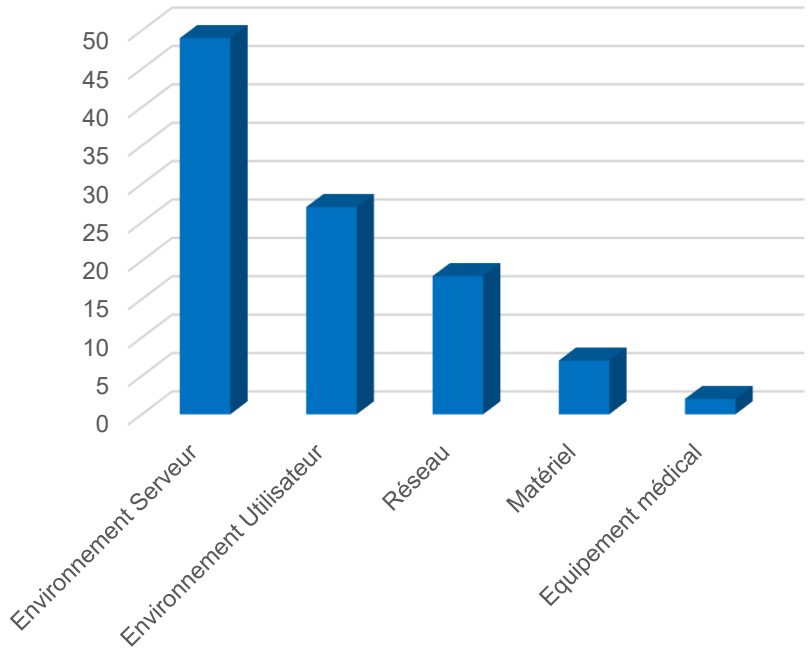
Nombre de CVE par éditeur

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

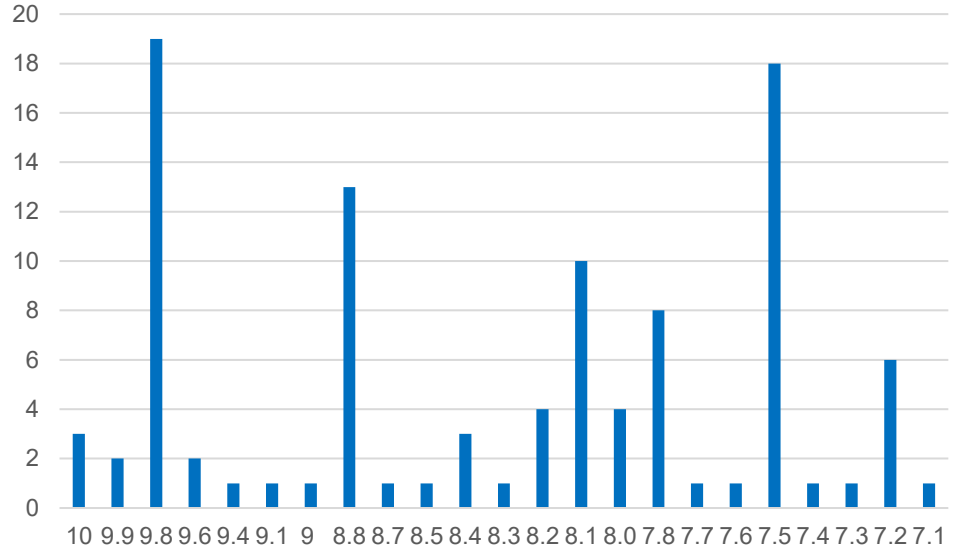


Nombre de CVE par catégorie de produit et score CVSS

CVE par catégorie de solution

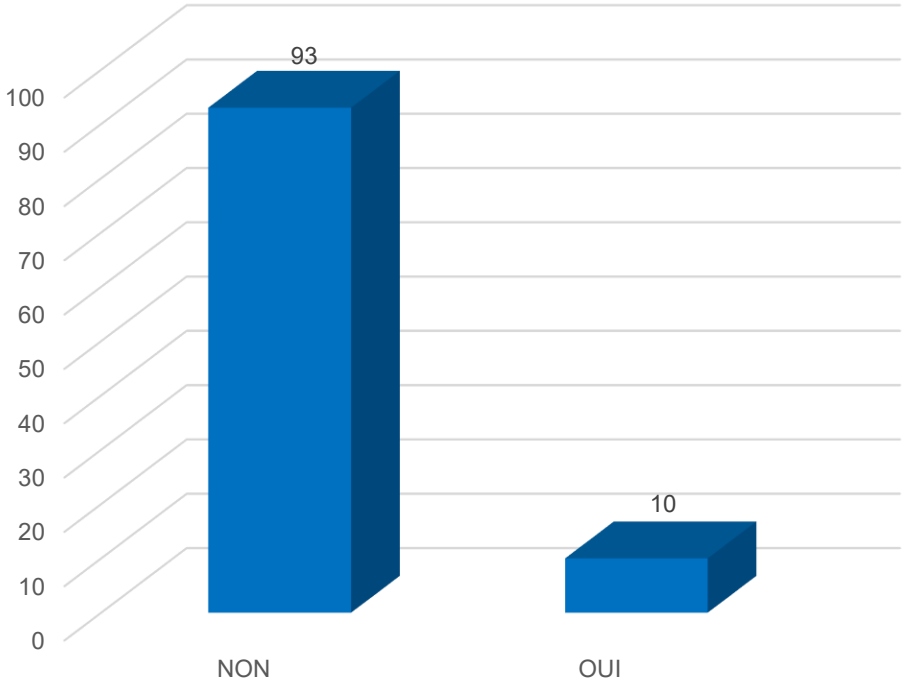


CVE par score CVSS

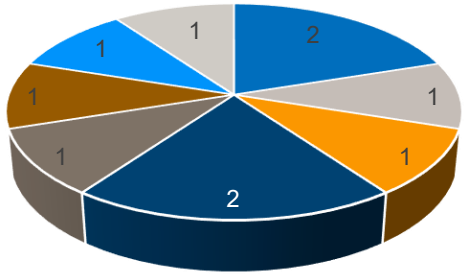


Vulnérabilités exploitées

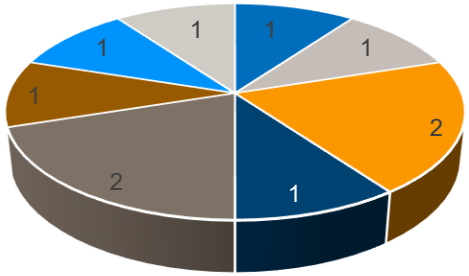
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par éditeur



Les vulnérabilités critiques à surveiller

9.8

GNU InetUtils

(CVE-2026-24061)

Contournement de la politique de sécurité

Exploitée

Un défaut de contrôle des données en entrée par le processus *telnetd* de GNU InetUtils permet à un attaquant non authentifié, en injectant une valeur spécifiquement forgée dans la variable d'environnement *USER*, de contourner l'authentification et d'obtenir un accès *root*.

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

9.8

Fortinet

(CVE-2026-24858)

Contournement de la politique de sécurité

Exploitée

Un défaut de contrôle des chemins dans FortiOS, FortiManager, FortiAnalyzer et FortiProxy permet à un attaquant, disposant d'un compte *FortiCloud* et d'un appareil enregistré, de se connecter à d'autres appareils enregistrés sous d'autres comptes si l'authentification *SSO FortiCloud* est activée sur ces appareils.

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

7.8

Microsoft

(CVE-2026-21509)

Contournement de la politique de sécurité

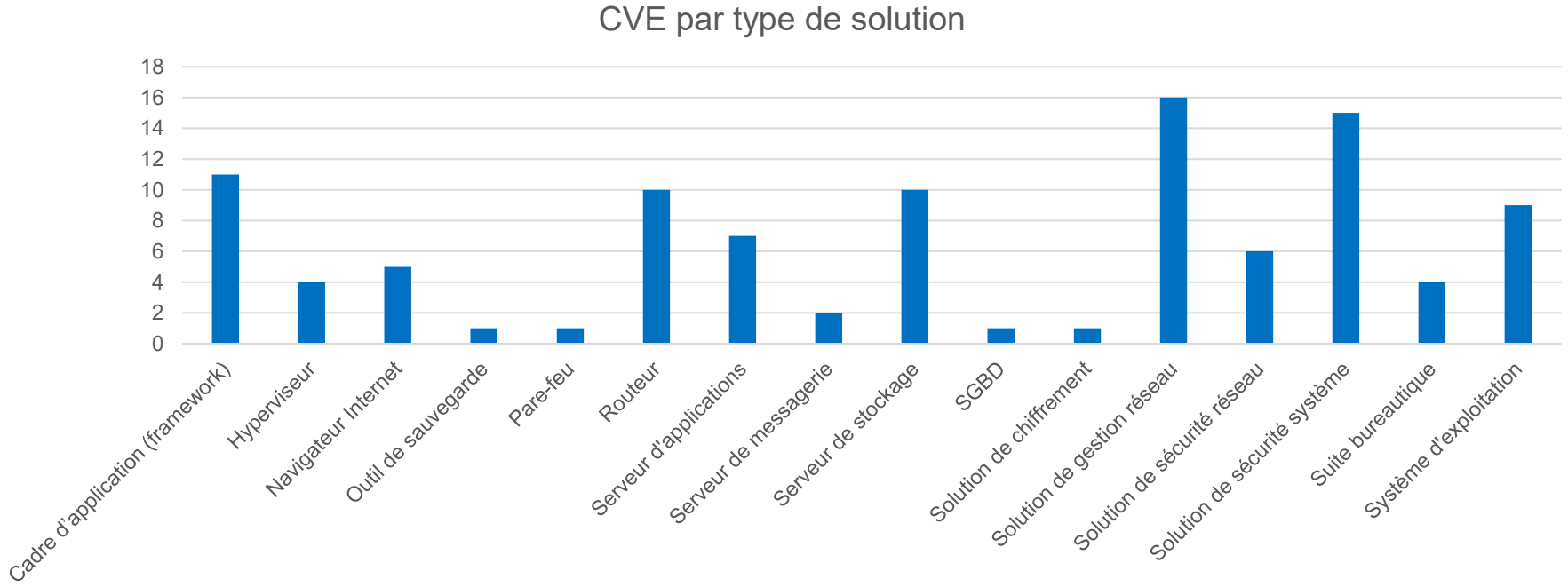
Exploitée

Un défaut de contrôle des entrées dans Microsoft Office permet à un attaquant, en persuadant une victime d'ouvrir un fichier spécifiquement forgé, de contourner la politique de sécurité.

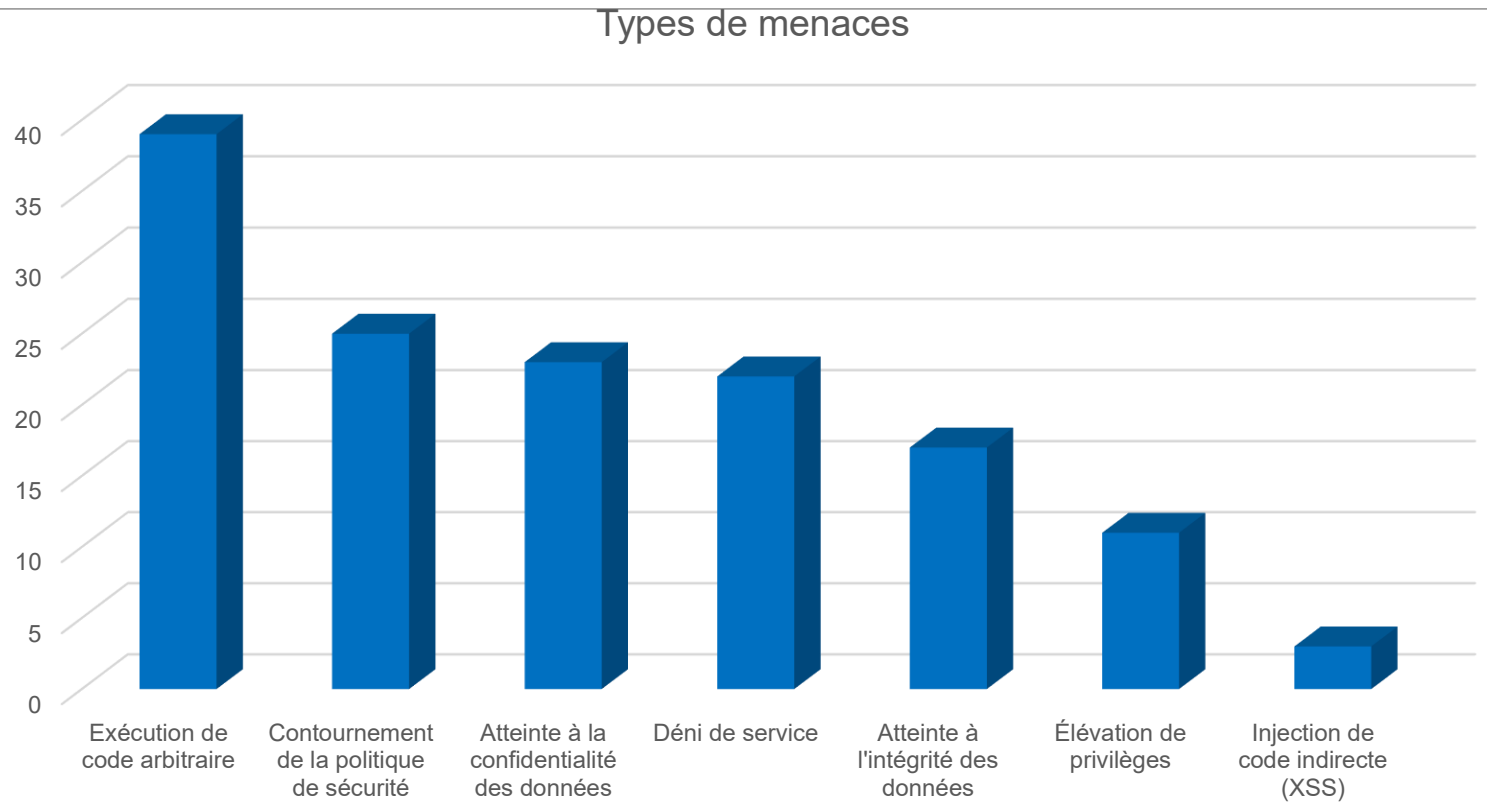
Recommandations : Appliquez les correctifs conformément aux instructions de l'éditeur.

Types de solutions vulnérables

Les solutions de gestion réseau, les solutions de sécurité système et les cadres d'application (framework) sont les principaux types d'équipements affectés par les vulnérabilités publiées.



Types de menaces



TOP 5 des failles selon le référentiel CWE