



La transformation commence ici 

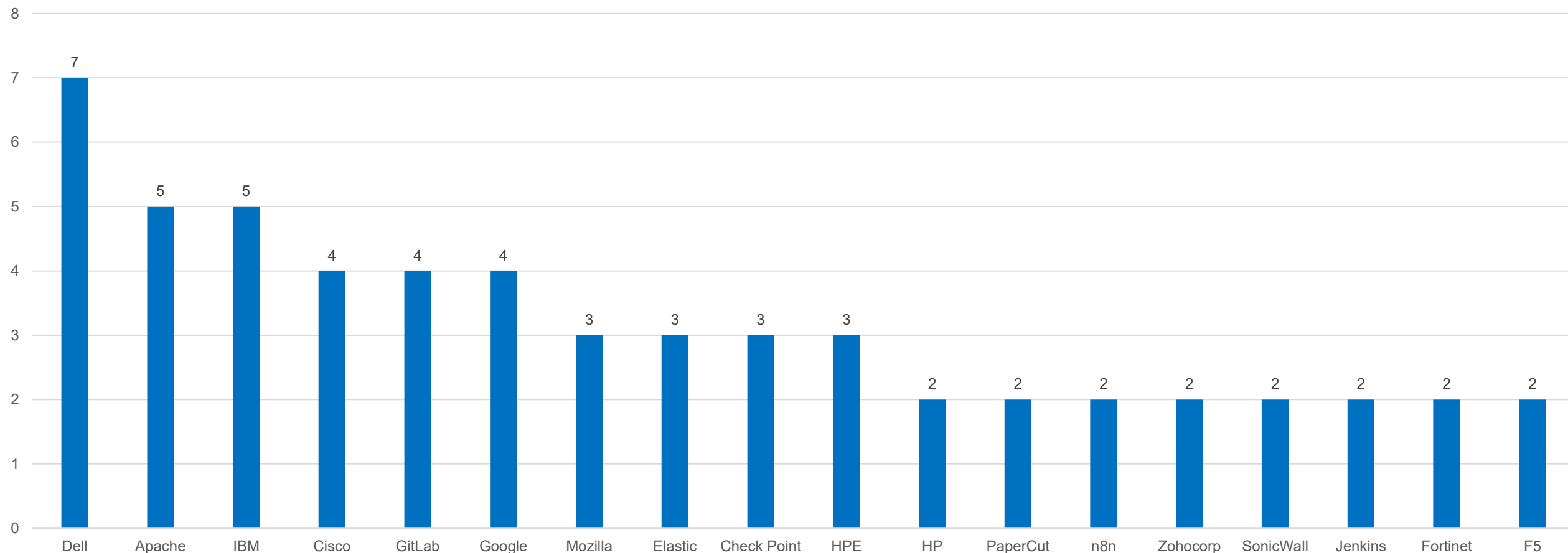


Indicateurs sur la publication des CVE pour le mois de septembre 2026

Nombre de CVE par éditeur

110 vulnérabilités ont été analysées et publiées (parmi lesquelles 13 alertes) sur le portail du CERT Santé.

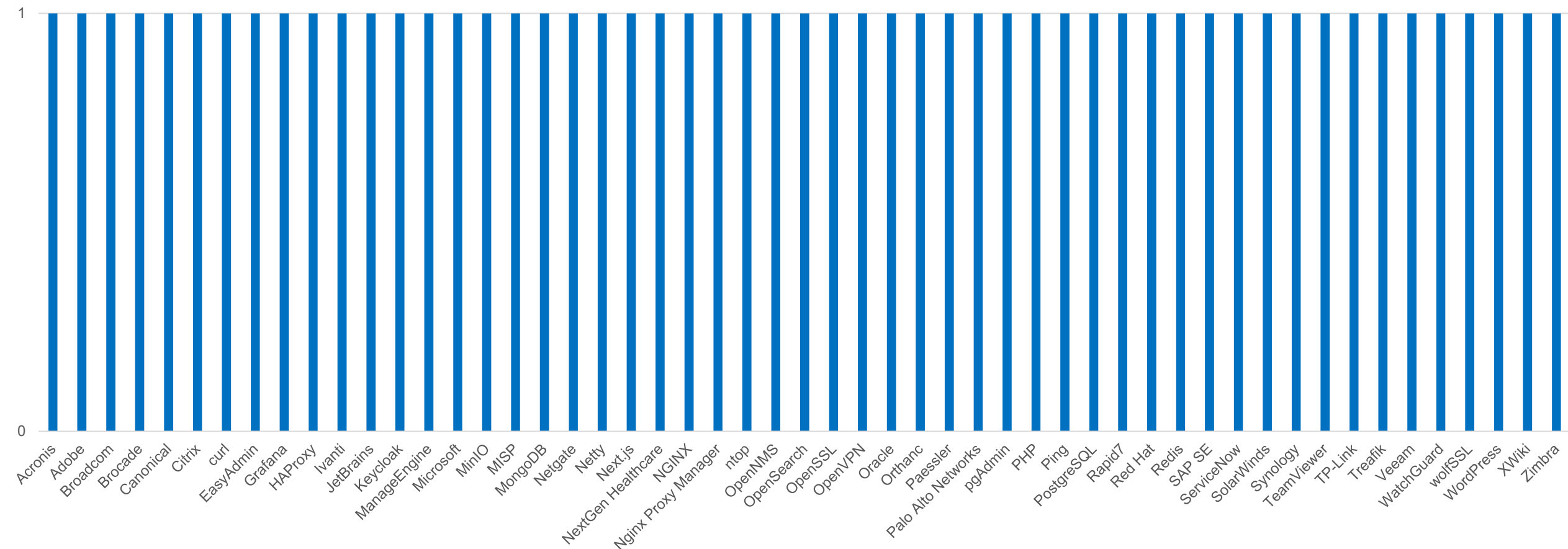
CVE par éditeur



Nombre de CVE par éditeur

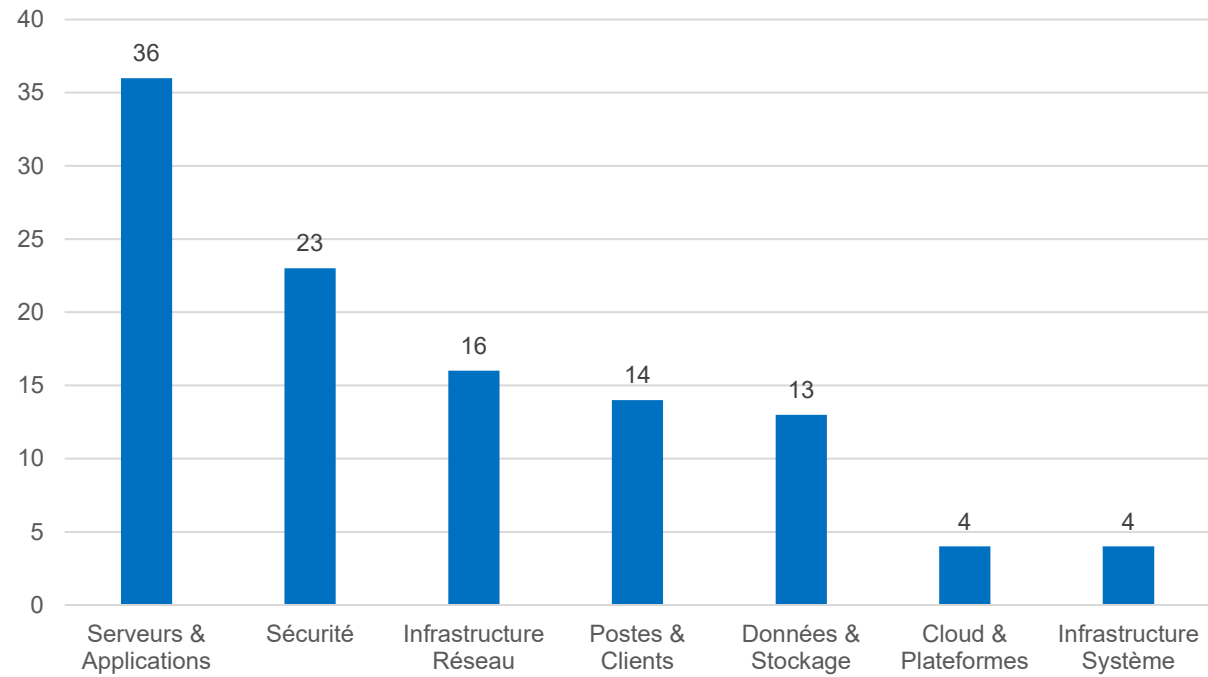
110 vulnérabilités ont été analysées et publiées (parmi lesquelles 13 alertes) sur le portail du CERT Santé.

CVE par éditeur

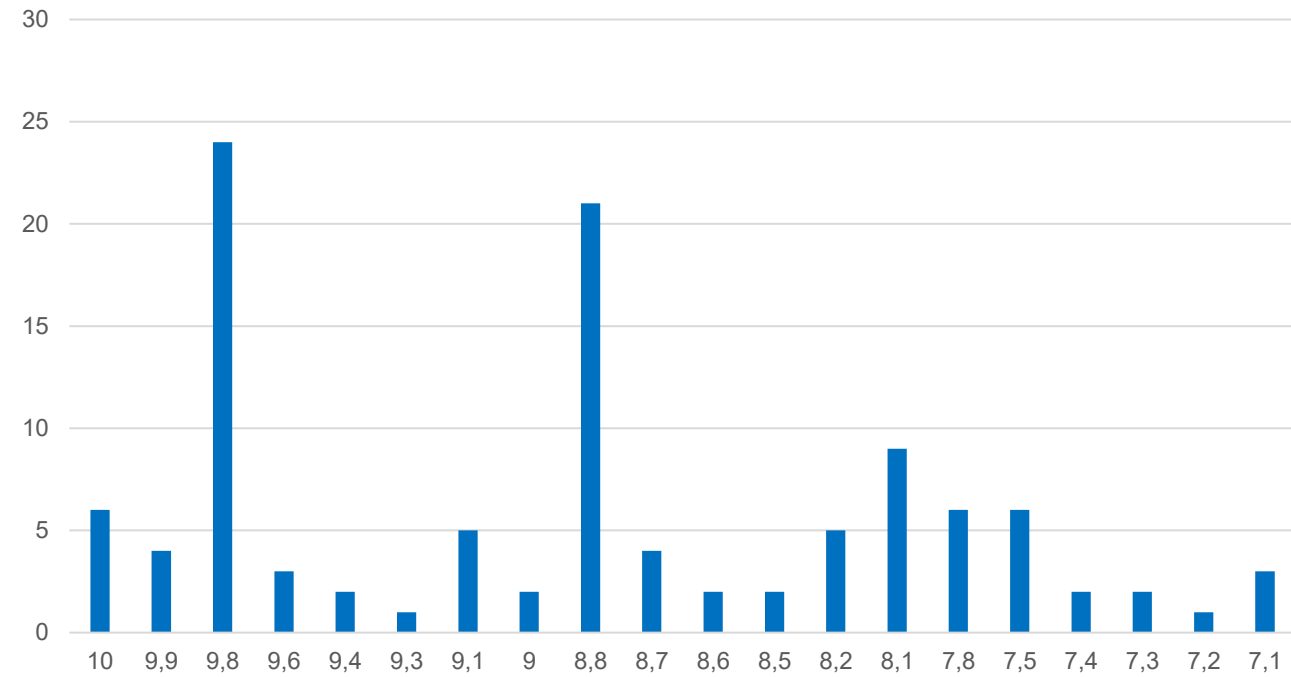


Nombre de CVE par catégorie de produit et score CVSS

CVE par catégorie de solution

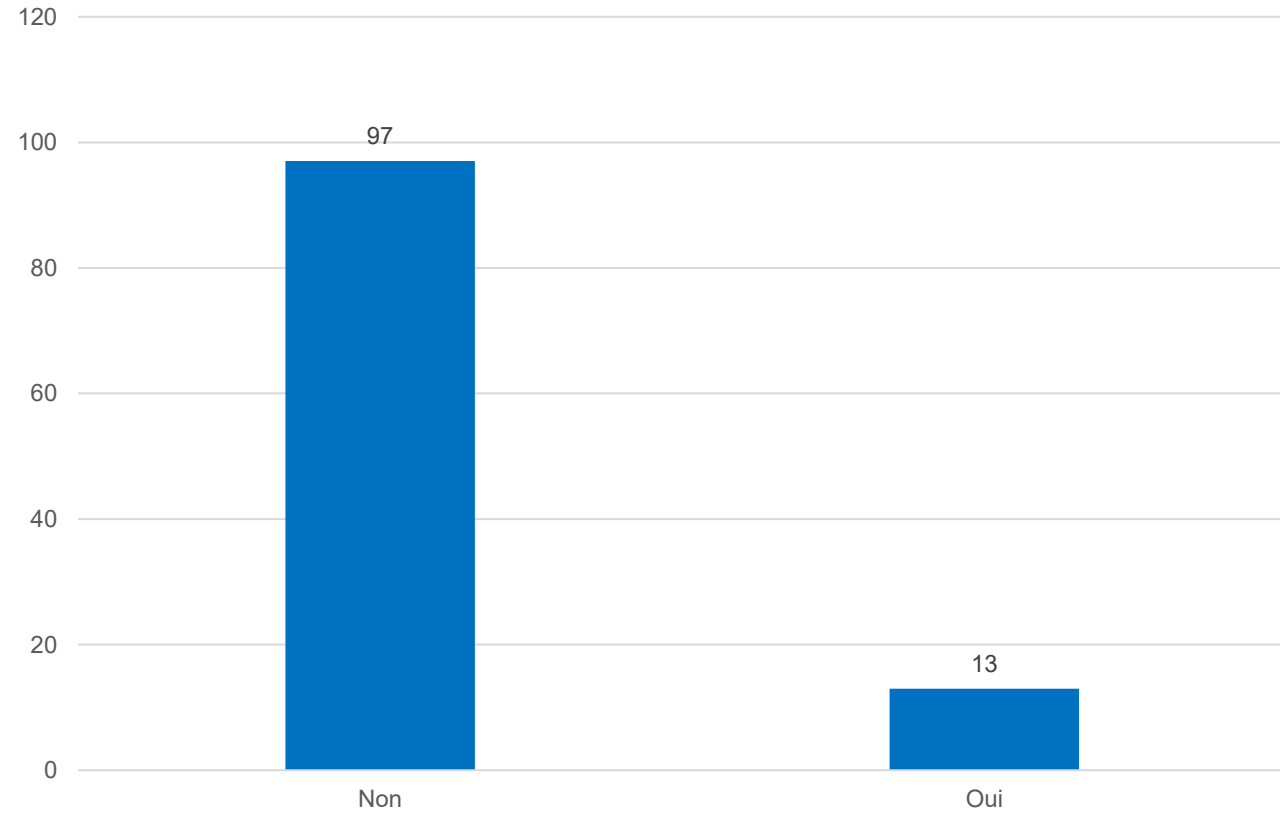


CVE par score CVSS

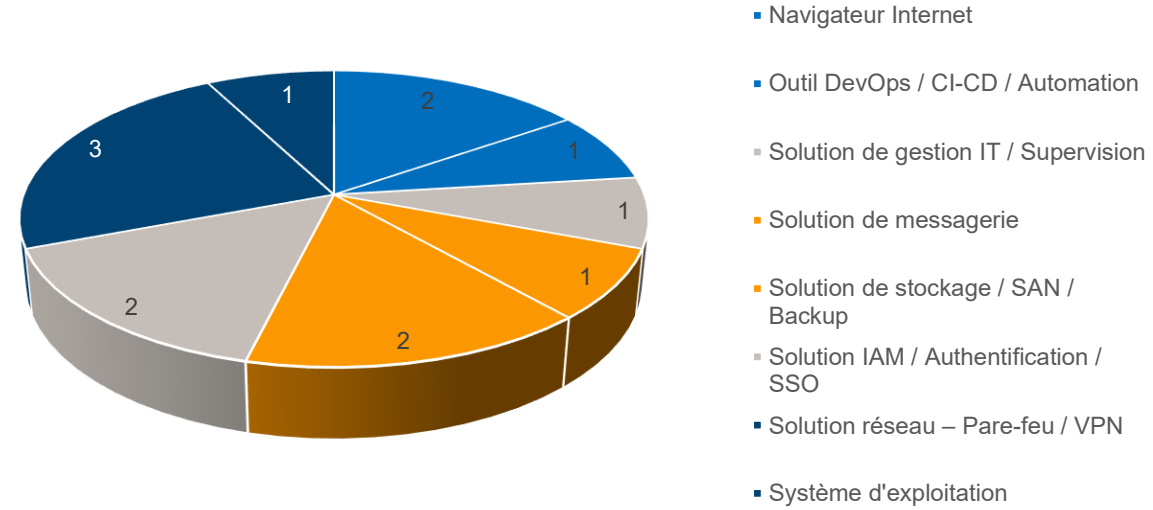


Vulnérabilités exploitées

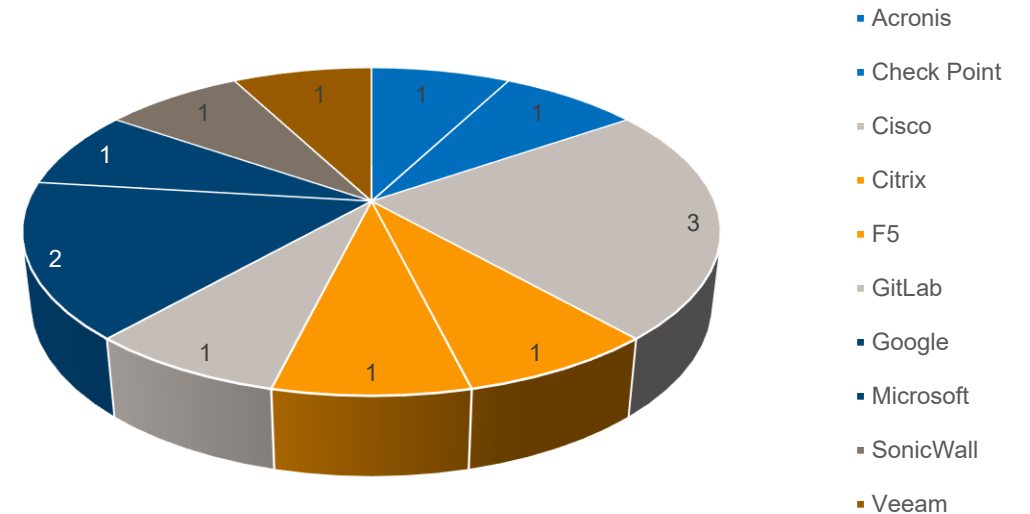
Failles exploitées



Failles exploitées par type de solution



Failles exploitées par produit



Les vulnérabilités critiques à surveiller

10

Cisco Secure Firewall MC ([CVE-2026-20079](#))

Exécution de code arbitraire

Exploitée

L'exploitation d'une vulnérabilité de **contournement d'authentification** (*authentication bypass*) affectant l'interface web de **Cisco Secure Firewall Management Center** permet à un attaquant distant non authentifié d'accéder, via des requêtes HTTP forgées, à un chemin d'exécution de scripts protégé. Il obtient ainsi l'exécution de code avec les privilèges root sur la console de gestion. Corrigée en mars, la faille est exploitée depuis l'été par plusieurs groupes, dont des acteurs étatiques et des groupes financiers, avec dépôt de web shells et d'outils de vol d'identifiants. Cette faille est inscrite au catalogue KEV de la CISA, avec preuve de concept publique disponible. Elle permet une **compromission totale de la console d'administration du parc de pare-feux**.

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

9.8

Citrix NetScaler ADC/Gateway ([CVE-2026-88771](#))

Exécution de code arbitraire

Exploitée

L'exploitation d'une vulnérabilité de **validation incorrecte des entrées** (*improper input validation*) affectant **NetScaler ADC** et **NetScaler Gateway** permet à un attaquant distant non authentifié d'injecter des commandes via des données contrôlées écrites dans les journaux, sans interaction utilisateur. Présente dans la configuration par défaut, elle a d'abord été exploitée comme zero-day dès début septembre dans des campagnes ciblées. Elle fait l'objet d'une exploitation de masse depuis la publication d'un PoC, avec dépôt de web shells sur les appliances non corrigées. Cette faille est inscrite au catalogue KEV de la CISA, avec preuve de concept publique disponible. Elle permet une **prise de contrôle à distance des appliances Citrix exposées**.

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

9.8

Check Point SM ([CVE-2026-93616](#))

Exécution de code arbitraire

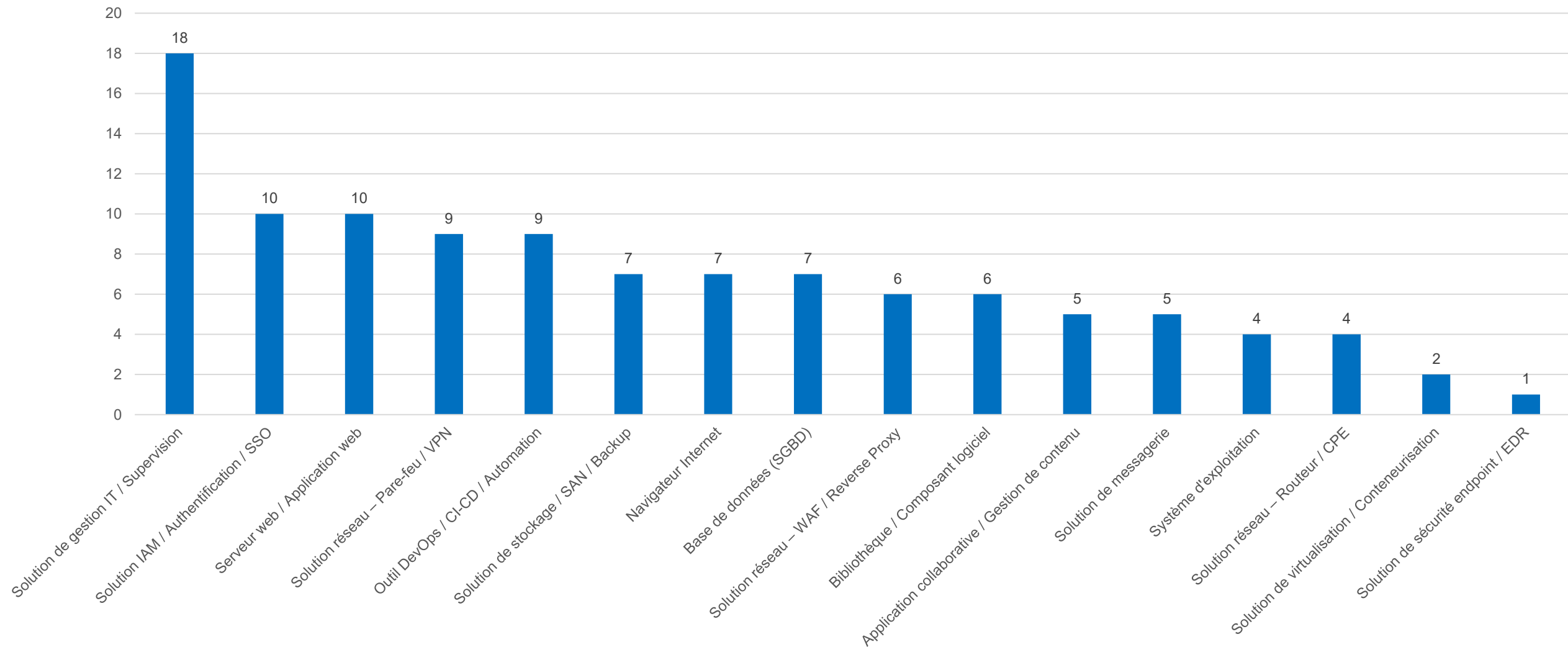
Exploitée

L'exploitation d'une vulnérabilité de **traversée de répertoire** (*path traversal*) affectant le service web d'administration de **Check Point Security Management** permet à un attaquant distant non authentifié de téléverser un script vers un chemin arbitraire du serveur, puis de l'exécuter via le port TCP/19009. Exploitée comme zero-day depuis le 23 juillet, soit 61 jours avant la publication du correctif, elle expose le serveur qui centralise les politiques, les identifiants administrateur et l'autorité de certification des passerelles. Cette faille est exploitée activement, avec preuve de concept publique disponible. Elle permet une **prise de contrôle du serveur de management et de la politique de sécurité de tout le parc Check Point**.

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

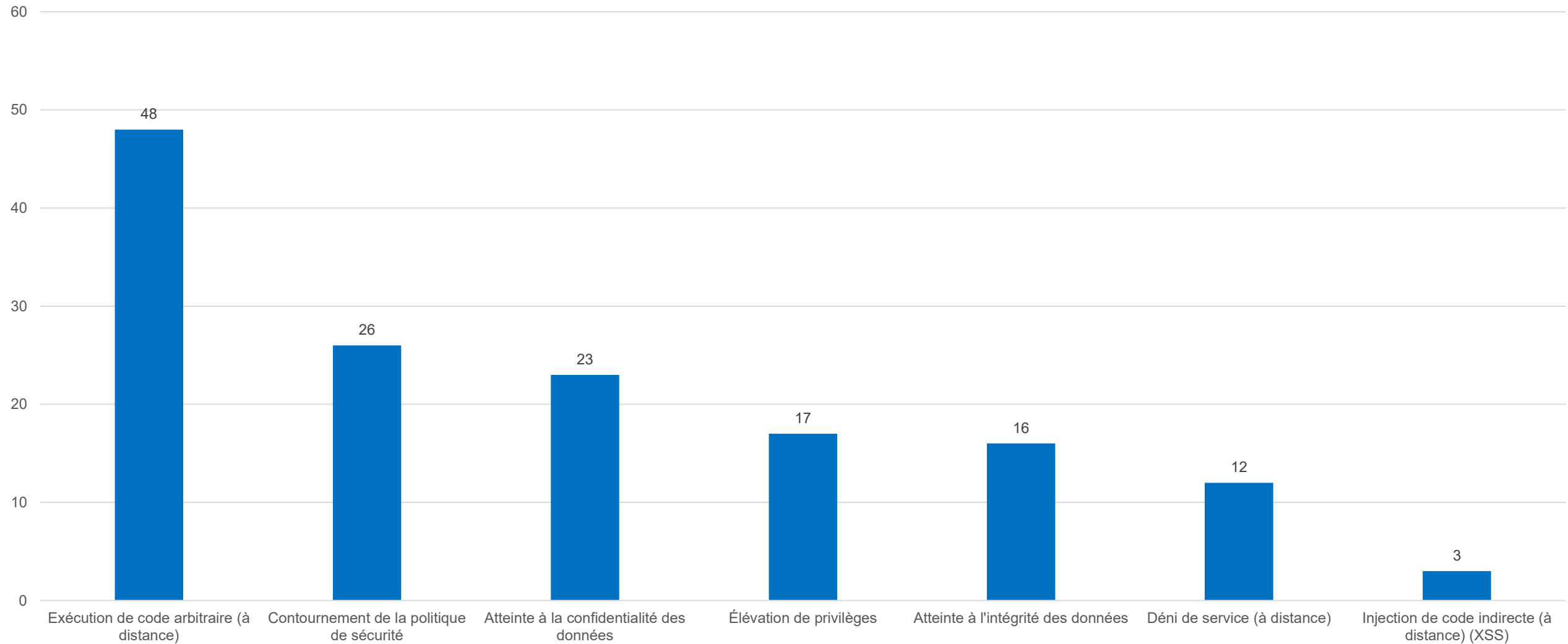
Types de solutions vulnérables

CVE par type de solution



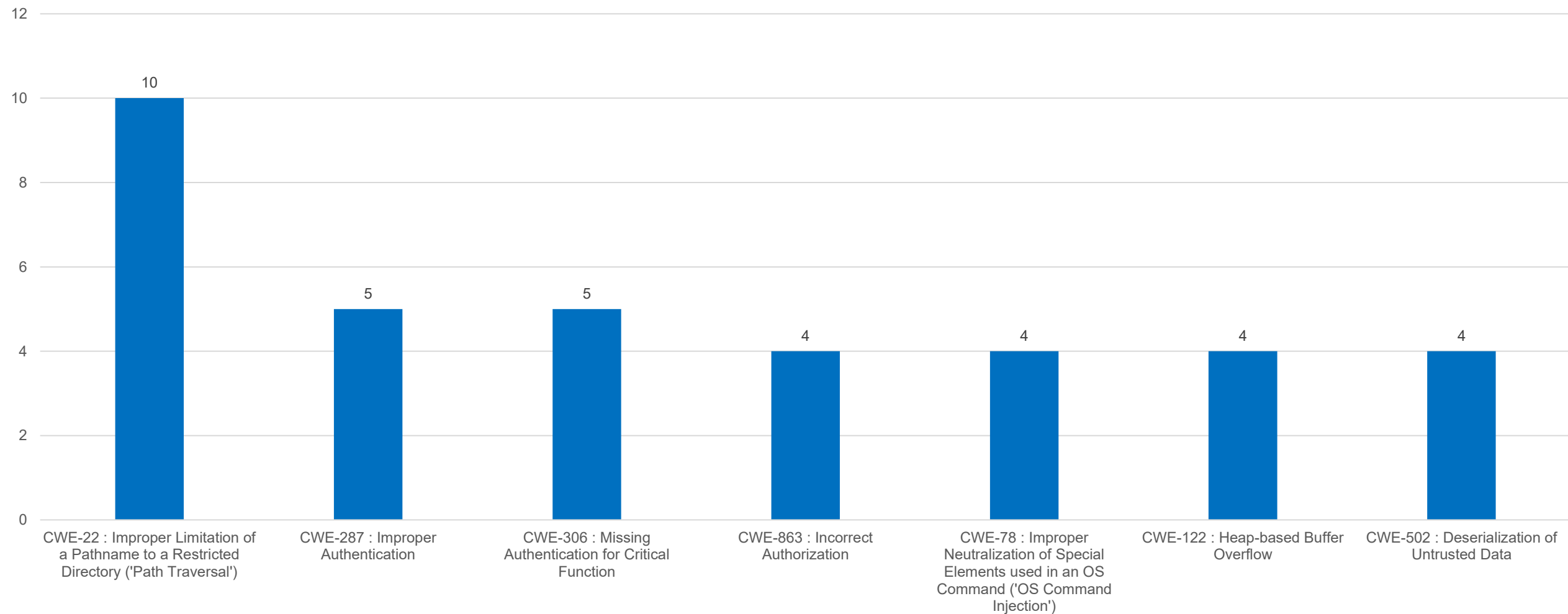
Types de menaces

Types de menaces



TOP 5 (7) des failles selon le référentiel CWE

Nombre de CVE par CWE



| Indicateurs mensuels sur les vulnérabilités