

Liste des vulnérabilités (vuln-type) – FortiGate IPS

Voici la liste des vulnérabilités (vuln-type) disponibles dans la configuration IPS de FortiGate, avec une explication claire et concrète de chaque type, utile pour adapter tes capteurs IPS à des menaces spécifiques :

ID	Vuln-Type	Description
1	N/A	Aucune catégorie spécifique – utilisé pour des signatures génériques.
2	DoS (Denial of Service)	Tentatives de rendre un service indisponible (crash, surcharge de ressources).
3	Buffer Errors	Dépassements de mémoire tampon qui permettent souvent l'exécution de code arbitraire.
4	Numeric Errors	Problèmes liés aux conversions ou calculs numériques (ex: débordement d'entier).
5	CSRF (Cross-Site Request Forgery)	Attaque visant à forcer un utilisateur authentifié à effectuer une action non souhaitée (surtout côté web).
6	XSS (Cross-Site Scripting)	Injections de scripts malveillants dans des pages web.
7	Path Traversal	Accès non autorisé à des fichiers sur le système via manipulation de chemins (../..).
8	Code Injection	Injection de code dans des applications vulnérables (ex: PHP, Python).
9	SQL Injection	Insertion de requêtes SQL malveillantes pour manipuler ou voler les données d'une base.
10	Format String	Vulnérabilités liées à une mauvaise gestion des chaînes formatées (printf() par exemple).
11	Malware	Signatures liées à des

		comportements ou fichiers malveillants (virus, trojans, etc.).
12	Anomaly	Comportements réseau suspects ou irréguliers (ex: scans, séquences TCP anormales).
13	Improper Authentication	Vulnérabilités dans les processus d'authentification (bypass, authentification faible...).
14	Information Disclosure	Fuite d'informations sensibles (versions de logiciels, configurations, erreurs affichées...).
15	Permission/Privilege/Access Control	Faibles permettant une élévation de privilèges ou accès non autorisé à des ressources.
16	OS Command Injection	Injection de commandes système dans des applications vulnérables.
17	Resource Management Errors	Mauvaise gestion des ressources (fichiers, mémoire, connexions...) entraînant des bugs ou vulnérabilités.
18	Other	Toutes autres vulnérabilités non classées dans les catégories précédentes.