CVSS (Common Vulnerability Scoring System) : système d’évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables

Métrique de base :

|  |  |  |
| --- | --- | --- |
| **Vecteur d’accès** | | |
| Local (L) | Accès physique ou compte local requis | 0,395 |
| Réseau local (A) | Accès au domaine de diffusion/collision (niveau 2 OSI) | 0,646 |
| Réseau (N) | Accès niveau 3 OSI ou supérieur, exploitable à distance | 1,000 |
| **Complexité d’accès** | | |
| Haut (H) | Conditions nécessitant une méthode facilement détectable par du personnel compétent | 0,350 |
| Moyen (M) | Nécessite une configuration non-commune, différente de celle par défaut | 0,610 |
| Bas (L) | Configuration par défaut, absence de conditions d’accès particulière | 0,710 |
| **Authentification** | | |
| Multiple | L’attaquant doit s’authentifier au moins 2 fois (même si le même authentifiant est utilisé | 0,450 |
| Simple | L’attaquant doit s’authentifier une seule fois | 0,560 |
| Inexistant | Aucune authentification requise | 0,704 |

Métrique d’impact :

|  |  |  |
| --- | --- | --- |
| **Confidentialité** | | |
| Aucun (N) | Aucun impact sur la confidentialité | 0,000 |
| Partiel (P) | Seule une partie de l’information est disponible | 0,275 |
| Complet (C) | Diffusion complète de l’information | 0,660 |
| **Intégrité** | | |
| Aucun (N) | Aucun impact sur l’intégrité | 0,000 |
| Partiel (P) | L’étendue de la modification d’intégrité est limitée | 0,275 |
| Complet (C) | Perte totale d’intégrité | 0,660 |
| **Disponibilité** | | |
| Aucun (N) | Aucun impact sur la disponibilité | 0,000 |
| Partiel (P) | Baisse de performances ou perte de quelques fonctionnalités | 0,275 |
| Complet (C) | Perte totale de disponibilité | 0,660 |

Métrique temporelle : évolue au fil des développements d’exploits et des mesures d’atténuation et correctifs.

Métrique environnementale : mesure subjective du risque dans le contexte par les parties concernées (propre à chaque organisation).

La mesure CVSS 3.0 prend en compte la métrique du périmètre et de l’interaction utilisateur, et ajoute la prise en charge des privilèges requis dans l’authentification. Elle ajoute la sévérité « Critique » aux niveaux de sévérité CVSS.

Association d’un niveau de sévérité à un score CVSS :

|  |  |  |  |
| --- | --- | --- | --- |
| **Score CVSS 2.0** | **Sévérité** | **Score CVSS 3.0** | **Sévérité** |
| 0,0 – 3,9 | Faible | 0,0 | Aucun |
| 0,1 – 3,9 | Faible |
| 4,0 – 6,9 | Moyen | 4,0 – 6,9 | Moyen |
| 7,0 – 10,0 | Élevé | 7,0 – 8,9 | Élevé |
| 9,0 – 10,0 | Critique |

Exemple de réactivité cohérente par rapport aux sévérités CVSS :

|  |  |  |  |
| --- | --- | --- | --- |
| **Sévérité** | **Mise à jour** | **Sévérité** | **Mise à jour** |
| Faible | 1 mois | Aucun | 1 mois |
| Faible | 1 mois |
| Moyen | 2 semaines | Moyen | 2 semaines |
| Élevé | 3 jours | Élevé | 1 semaine |
| Critique | 3 jours |