Common Vulnerabilities and Exposures

Une cve par jour éloigne le sysadmin

CC BY-SA Typhlos

CVE, késaco ?

- Système pour rassembler et normaliser les failles des systèmes et des produits très utilisés à travers le monde notamment via un score le CVSS
- Créé en septembre 1999 et géré par Mitre Corporation, fondation à but non lucratif
- Attribue un score à chaque vulnérabilité pour classifier sa dangerosité

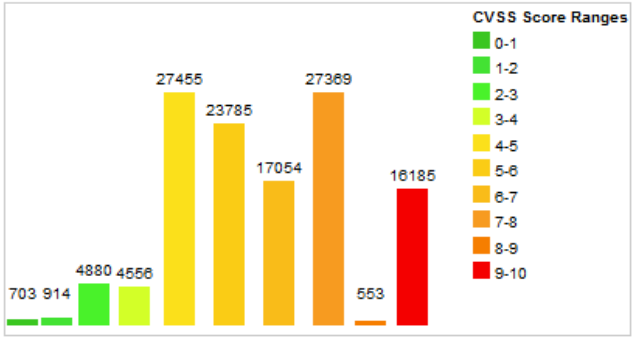
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Weighted Average CVSS Score: **6.6**

Vulnerability Distribution By CVSS Scores



Tout publier ou non ?

- Lister les failles publiquement, parfois même avec des exploits, est-ce une bonne idée ?
  - Eternel débat de la sécurité par l'obscurité vs sécurité par la transparence
- Au départ, les entreprises ne s'intéressaient pas du tout à corriger des failles
  - Publier les failles en publiques obligent les entreprises à les prendre en compte
  - Liste historique : Bugtraq depuis 1993
- Bonnes pratiques :
  - Contacter d'abord le ou les devs pour les informer
  - Attendre un correctif en mettant ou non une deadline
  - Publier la faille avec généralement un Proof of Concept

Quand on peut être fier d’avoir un 0

- Score de 0 à 10 déterminé selon plus catégories :
  - Vecteur d’attaque : physique, local, à distance
  - Complexité de l’attaque
  - Privilèges requis pour l’attaque
  - Nécessité d’une interaction de l’utilisateur
  - Portée de l’attaque
  - Impact sur la confidentialité
  - Impact sur l’intégrité
  - Impact sur la disponibilité
- D’autres facteurs peuvent jouer sur la note

Panic button

- Concrètement le score indique la sévérité de la faille :
  - < 4 : faible
  - Entre 4 et 7 : modéré
  - Entre 7 et 9 : élevé
  - < 9 : critique, là on peut paniquer (ou pas)
- Le score n’est qu’un indicateur, il faut aussi prendre en compte le contexte

Un exemple : Log4Shell

- CVE 2021-44228
- Score 10/10 :
  - Impact très vaste et exploitée très facile
- Détecté le 24/11/2021
- Correction avec la 2.15.0 le 09/12/2021
- Faille publiée dans la foulée

Comment tout casser ?

- Comment exploiter des CVEs ?
- 1ère étape : récupérer des informations
  - linpeas, linux exploit suggester, cve.mitre.org …
- 2ème étape : chercher un exploit
  - exploit-db.com, github, metasploit …
- 3ème étape : exploiter
- 4ème étape : ???
- 5ème : profit
- Si pas d'exploit, il va falloir se retrousser les manches et en écrire un