# Qu’est-ce qu’une faille de sécurité ?



Une faille de sécurité ou vulnérabilité informatique concerne toute faiblesse d’un système (ex : un logiciel), qui permettrait à une personne malveillante de l’exploiter et d'altérer le fonctionnement du système ou encore d'accéder à des données sensibles. Une faille est généralement involontaire et peut résider dans la conception du logiciel ou un problème plus profond au niveau matériel, certaines failles ne peuvent être corrigées compte tenu de la spécificité du matériel, du logiciel, du protocole...

# Qu’est-ce qu’une vulnérabilité CVE ?

Le système CVE (Common Vulnérabilités and Exposures) permet de recenser toutes les failles et les menaces liées à la sécurité des systèmes d’information. Pour ce faire, un identifiant unique est attribué à chaque faille.

Les failles de sécurité informatique sont identifiées par un identifiant unique composé de l'année de découverte et du numéro d'identification de l'organisme. Une faille qui est détectée mais qui n'a pas encore été publiée est appelée "0 day".

Après avoir découvert une faille, l'entreprise peut demander à la partie concernée si elle accepte la faille. Si c'est le cas, elle soumet la faille à l'organisation MITRE qui décidera de la publier ou non, en fonction de la notoriété et de l'utilisation du logiciel. MITRE attribue un identifiant unique CVE à la faille, et l'entreprise doit remplir un formulaire détaillant la faille. Elle peut également contacter la personne ou l'entreprise qui a découvert la faille.

# Les Différents Types et Niveaux des Failles

Les failles de sécurité peuvent toucher tous les aspects de l'informatique, des protocoles réseau aux logiciels, en passant par les CMS et les langages de programmation. Leur gravité est évaluée sur une échelle de 1 à 10 grâce au système de notation CVSS, qui prend en compte des facteurs temporels comme la divulgation, l'exploitation et les contre-mesures.

# OWASP

OWASP est une communauté en ligne dédiée à la cybersécurité, fournissant des recommandations et des outils pour évaluer et améliorer la sécurité des applications web. Créée en 2001, la communauté propose des informations et des solutions aux développeurs pour sécuriser leurs applications web, notamment avec le Top 10 OWASP.

# Exemples de vulnérabilités

CVE-2021-4034 :

Faille de sécurité nommée Pwnkit dans pkexec découverte en 2021 par Qualys. Existe depuis 12 ans sur toutes les distributions Linux. Niveau de criticité : 7.5/10.

Pkexec, inclus dans le paquet Polkit (anciennement PolicyKit), gère les politiques pour les processus avec droits restreints à communiquer avec des services privilégiés du système. Créé pour exécuter des actions nécessitant des privilèges élevés.

Pkexec est une alternative à sudo qui permet à un utilisateur autorisé d'exécuter une commande en tant qu'un autre utilisateur.

La faille permet une élévation de privilèges, donnant à un utilisateur authentifié les droits d'administrateur pour exécuter des commandes en tant que root.

La vulnérabilité provient d'un problème de corruption de mémoire dans pkexec, une commande en langage C qui gère mal les arguments en ligne de commande. L'attaquant peut dépasser la mémoire allouée et écrire des commandes en dehors de cet espace, ce qui permet une élévation de privilèges en tant que root. Pour protéger son serveur Linux, il faut appliquer le patch correctif ou supprimer les droits de pkexec en utilisant la commande "chmod 0755 /usr/bin/pkexec".

# Qu’est-ce que Log4J et Log4Shell ?

Log4J est une bibliothèque d'Apache pour gérer les logs d'applications. Log4Shell est une vulnérabilité critique détectée en novembre 2021 dans Log4J, la plus populaire bibliothèque de logs utilisée dans les applications. Son niveau de criticité est évalué à 9.3/10 sur cvedetails.com et 10/10 sur le site officiel d'Apache. L'ANSI a également publié un avertissement sur cette faille sur son site.

En quoi consiste Log4Shell ?

Log4Shell est une vulnérabilité critique qui permet l'exécution de code à distance dans Log4J. Un attaquant peut télécharger des virus, installer des logiciels malveillants ou prendre le contrôle du serveur à distance. Log4J se connecte à des serveurs extérieurs via la fonction "jndi" sans effectuer de contrôle sur les données récupérées, ce qui permet l'injection de code malveillant. La mise à jour vers Log4J 2.15.0 corrige cette faille, mais d'autres vulnérabilités ont été découvertes dans les patchs de correction. Un attaquant peut également combiner Log4Shell avec d'autres failles, comme Pwnkit, pour obtenir des privilèges root sur un système ciblé et exécuter des commandes sur n'importe quelle machine.

# Les conséquences des failles de sécurités.

Les vulnérabilités sont généralement corrigées rapidement une fois découvertes, mais il peut y avoir un délai entre leur découverte par la victime et leur correction, ce qui laisse aux attaquants le temps de les exploiter. Par exemple, la faille Pwnkit a été découverte après 12 ans et potentiellement exploitée par plusieurs attaquants avant d'être identifiée. Les conséquences des failles peuvent être graves pour les individus et les entreprises, telles que la fuite d'informations confidentielles ou l'indisponibilité des systèmes, entraînant des coûts importants.