Vulnérabilités, exploits et attaques zéro-day

Pr Chérif DIALLO, CISSP
Professeur Titulaire des Universités
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept. Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

"Si la science évolue, c'est souvent parce qu'un aspect encore inconnu des choses se dévoile soudain." François Jacob / Le Jeu des possibles.

Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui un problème crucial de cyber sécurité. Il s'agit des vulnérabilités et menaces zéro-day. Ces dernières années, les vulnérabilités et menaces zéro-day ont considérablement augmenté et causé des dommages de plus en plus importants. Ainsi, elles deviennent une priorité parmi les priorités dans la gestion des risques cyber. Après une brève définition, ce bulletin, donne quelques exemples de vulnérabilité zéro-day et d'attaques zéro-day, leur mode de fonctionnement et les solutions face à ces menaces.

Mots clés : Vulnérabilité zéro-day, Exploit zéro-day, Attaque zéro-day.

---

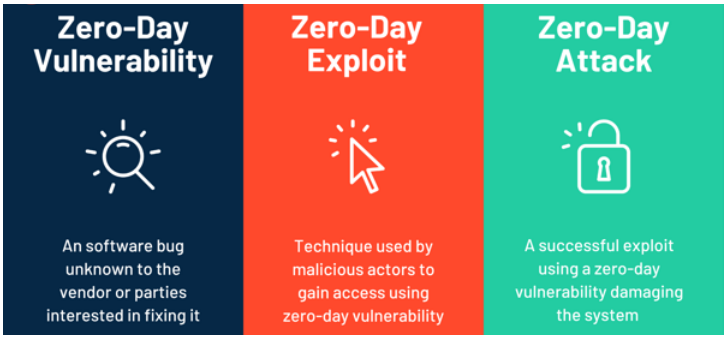
1. Définition

Selon son étymologie, le mot « Vulnérabilité » vient du latin « Vulnerare », qui signifie blesser, endommager, entamer, porter atteinte à, faire mal à, froisser, offenser. La vulnérabilité est donc le caractère de ce qui est fragile, précaire, de ce qui peut être attaqué, blessé, endommagé.

Une vulnérabilité informatique est un défaut de sécurité, une faille ou une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité, à la disponibilité ou à l'intégrité des données qu'il contient. Ces failles proviennent d'origines multiples parmi lesquelles on peut citer trois causes fondamentales : (i) les vulnérabilités inhérentes, (ii) les faiblesses technologiques et (iii) les défauts de configuration (par exemple : l'utilisation des mots de passe par défaut non modifiés).

En cyber sécurité, une vulnérabilité zéro-day, quant à elle, est une faille passée inaperçue dans une application ou un système d'exploitation, qui n'est pas connu publiquement et dont le fournisseur n'a pas connaissance. Pour une vulnérabilité zéro-day, il n'existe pas encore de défense ni de correctif parce que, tout simplement, le fabricant du logiciel impacté ignore son existence, et par conséquent n'a pas eu de temps (zéro jour) pour préparer une solution efficace.

Une vulnérabilité zéro-day constitue donc une menace potentielle, une faille de sécurité qui subsiste tant qu'elle n'a pas été réparée. Mais avant qu'un correctif ne soit développé, testé et publié, il existe une période critique pendant laquelle la vulnérabilité peut être exploitée pour perpétrer une attaque. Durant cet intervalle, les attaquants ont un bref avantage, car les logiciels malveillants sont souvent plus faciles et plus rapides à concevoir. La vulnérabilité perd son caractère zéro-day dès qu'elle est connue publiquement ou par le fournisseur.

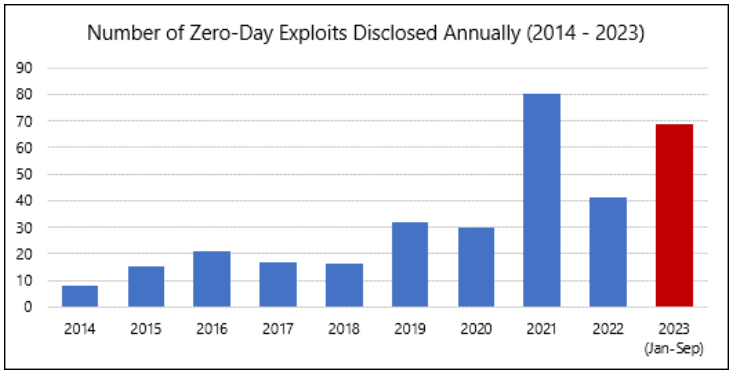


Un exploit zéro-day est le pire des scénarios, dans lequel un code malveillant est développé et déployé pour tirer parti de la vulnérabilité avant qu'une réponse de sécurité ne soit disponible.

Une attaque zéro-day se produit lorsque des individus malveillants utilisent un exploit connu pour cibler un système vulnérable afin d'en perturber le fonctionnement ou de voler des informations importantes.

2. Quelques exemples de vulnérabilités zéro-day

Le nombre d'exploits de type zéro-day a explosé ces dernières années. Un nombre record de 83 exploits zéro-day a été signalé en 2021, ce qui représente plus du double du nombre signalé en 2020. Les chercheurs en sécurité attribuent cette augmentation du nombre d'événements zéro-day à la multiplication continue des offres logicielles, des services d'hébergement dans le cloud et des appareils connectés à Internet, mais aussi à la vigilance et à la sophistication croissantes des logiciels et services de sécurité, qui découvrent aujourd'hui des attaques qui auraient pu passer inaperçues auparavant. Voici quelques exemples célèbres d'attaques zéro-day récentes :



- ***Vulnérabilité zéro-day de Chrome (2021) :*** En 2021, Google Chrome a fait l'objet d'une série de menaces zéro-day ayant entraîné la publication de mises à jour par Chrome. La vulnérabilité provenait d'un bug dans le moteur JavaScript V8 utilisé dans le navigateur Web.
- ***Zoom (2020) :*** Une vulnérabilité a été identifiée sur la célèbre plateforme de vidéoconférence. Au cours de cette attaque zéro-day, les cybercriminels accédaient au PC d'un utilisateur à distance exécutant une ancienne version de Windows. Si la cible était un administrateur, le cybercriminel pouvait prendre le plein contrôle de sa machine et accéder à l'ensemble de ses fichiers.
- ***Apple iOS (2020) :*** Apple iOS est souvent décrit comme la plus sécurisée des grandes plateformes de smartphone. Toutefois, en 2020, le système d'exploitation a fait l'objet d'au moins deux séries de vulnérabilités zéro-day, notamment un bug zéro-day permettant aux cybercriminels de compromettre les iPhones à distance.
- ***Microsoft Windows, Europe de l'Est (2019) :*** Cette attaque se concentrait sur l'augmentation locale des droits, un domaine vulnérable de Microsoft Windows, et a ciblé des institutions gouvernementales d'Europe de l'Est. La faille d'exploitation zéro-day a profité d'une vulnérabilité de droits locale de Microsoft Windows pour exécuter un code arbitraire, installer des applications, puis afficher et modifier les données sur les applications compromises. Une fois l'attaque identifiée et signalée au Centre de réponse aux problèmes de sécurité Microsoft, un correctif a été développé et déployé.
- ***Microsoft Word (2017) :*** Cette faille d'exploitation zéro-day a mis en péril des comptes bancaires personnels. Les victimes étaient des personnes qui avaient ouvert accidentellement un document Word malveillant. Le document affichait une invite « Charger le contenu distant », avec une fenêtre contextuelle demandant aux utilisateurs un accès externe depuis un autre programme. Lorsque les victimes cliquaient sur « Oui », le document installait un programme malveillant sur leur appareil, capable de capturer leurs informations de connexion bancaires.
- ***Sony Pictures (2014) :*** l'attaque zéro-day la plus célèbre a potentiellement mis le réseau Sony à l'arrêt et a conduit à la publication de ses données sensibles sur des sites de partage de fichiers. L'attaque, fin 2014, a vu la fuite d'informations sur les films à venir, les plans d'affaires de l'entreprise et les adresses e-mail personnelles des cadres supérieurs.
- ***RSA (2011) :*** Une autre attaque zéro-day très publique a vu les hackers utiliser une vulnérabilité non corrigée dans Adobe Flash Player pour accéder au réseau de la société de sécurité RSA en 2011. Les assaillants ont envoyé des e-mails joints à des feuilles de calcul Excel, qui contenaient un fichier Flash intégré qui exploitait la vulnérabilité zéro-day, aux employés de RSA. Lorsque les employés ont ouvert la feuille de calcul, ils ont donné à l'assaillant le contrôle à distance de l'ordinateur de l'utilisateur, qu'ils

avaient l'habitude de rechercher et de voler des données. Ces informations se sont révélées liées à ses produits, comme SecurID, que les employés utilisent pour accéder aux données sensibles.

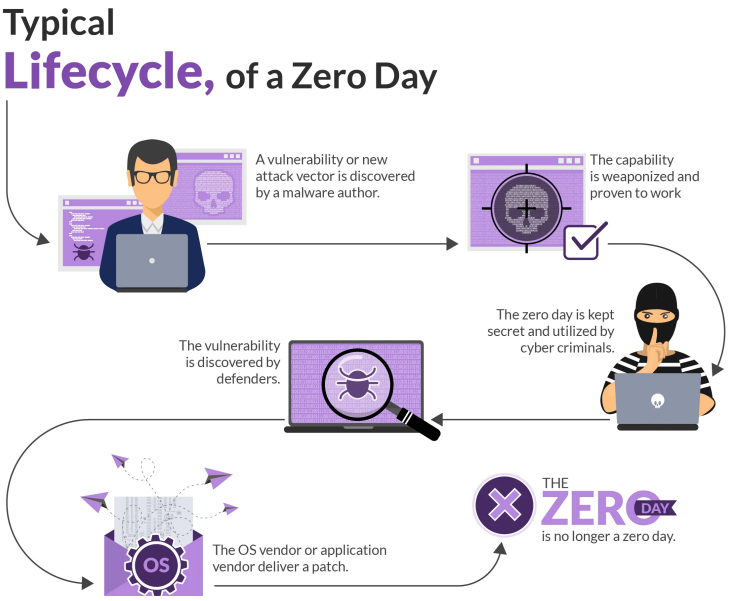
- ***Stuxnet (2010) :*** Stuxnet figure parmi les exemples les plus célèbres d'attaque zéro-day. Découvert pour la première fois en 2010, mais se répandant depuis 2005, ce ver informatique malveillant a affecté les ordinateurs du secteur de la fabrication exécutant un automate programmable industriel (API). Le ver ciblait principalement les usines iraniennes d'enrichissement de l'uranium dans le but d'interrompre le programme nucléaire du pays. Il a infecté les API en profitant des vulnérabilités du logiciel Siemens Step7. Les API ont alors exécuté des commandes inattendues sur les machines de la chaîne de montage. L'histoire de Stuxnet a fait ensuite l'objet d'un documentaire intitulé Zéro-Days.
- ***Opération Aurora (2009) :*** en 2009, un exploit zéro-day a ciblé la propriété intellectuelle de plus de 20 grandes organisations mondiales, dont Adobe Systems, Blackberry, Dow Chemical, Google, Morgan Stanley et Yahoo. Il a exploité les vulnérabilités d'Internet Explorer, de diverses autres versions logicielles Windows et de Perforce, que Google utilisait pour gérer son code source. L'attaque visait à accéder aux référentiels de code source et à les modifier dans les organisations de haute technologie.

3. Comment fonctionne une attaque zéro-day ?

Le chronogramme de l'exploitation « zéro-day » peut être subdivisé en plusieurs étapes :

- Une vulnérabilité dans un système, un logiciel ou un service est découverte par un individu ;
- Cette personne ne divulgue pas les détails de la vulnérabilité au fournisseur de manière responsable via le programme CVE, mais choisit plutôt de garder la connaissance de la vulnérabilité privée ;
- La connaissance de la vulnérabilité est ensuite utilisée soit par la personne qui la découvre, soit par un partenaire ou un contact pour développer un « code d'exploitation » capable d'exploiter la vulnérabilité ;
- Facultativement, l'exploit peut être vendu sur le dark web, sur le marché noir ou à une « plateforme d'acquisition d'exploit » plus légitime, ou encore les connaissances conservées uniquement par son découvreur ;
- L'exploit est ensuite utilisé pour effectuer une ou plusieurs attaques sur les systèmes vulnérables. Étant donné que l'effet de l'exploit peut ne pas être immédiatement reconnaissable ou détectable, un attaquant devra décider s'il doit tenter de maximiser les bénéfices à court terme de l'exploit (en effectuant une attaque de Ransomware voir [BMS1] ou similaire pour un gain financier immédiat) ou peut-être choisir d'adopter une vision à plus long terme et de « développer » l'ancrage qu'il a établi dans un système ou une organisation cible.

Ces exploits sont considérés comme « zéro-day » avant le jour où le fournisseur est informé de l'existence de l'exploit ; « zéro » faisant référence au nombre de jours depuis que le fournisseur a découvert la vulnérabilité. Le « jour zéro » est le jour où le fournisseur prend connaissance de la vulnérabilité et commence à travailler sur un correctif.



4. Solutions : comment se protéger contre les attaques zéro-day ?

Même si cela peut paraitre difficile, il existe néanmoins des mesures que les organisations peuvent prendre pour prévenir, détecter ou corriger les attaques zéro-day :

- ***Minimiser la « surface d'attaque » de votre organisation*** en veillant à renforcer les systèmes en réduisant leur empreinte réseau, en limitant les ports, services et logiciels disponibles et en cours d'exécution à ceux qui sont essentiels ;
- Exposer les services individuels uniquement aux systèmes et aux utilisateurs qui ont un besoin professionnel d'y accéder, en utilisant un pare-feu intelligent ;
- Filtrer les classes de vulnérabilités en utilisant un pare-feu applicatif pour tous les services sensibles ;
- ***Restreindre la capacité de rebond d'un attaquant*** qui compromettrait un système à « pivoter » son attaque et à rebondir sur d'autres systèmes via un mouvement latéral avec une segmentation robuste et un réseau verrouillé ;
- Dans la mesure du possible, compte tenu des contraintes de budget et d'échelle, ***envisager d'utiliser plusieurs couches de dispositifs tels que des firewalls (i.e. pare-feu) de différents fournisseurs***, de sorte que même si l'une d'elles est vulnérable, la « couche » suivante peut ne pas l'être ;
- ***Tenir compte du principe de « défense en profondeur »*** dans toute décision relative à l'architecture du système, en vous assurant que vous ne comptez pas sur une seule mesure préventive comme panacée totale contre les menaces, mais que vous exploitez plusieurs niveaux de défense ;
- ***Mettre en œuvre une journalisation et un audit robustes*** et garantir que les journaux sont stockés hors système de manière immuable (non modifiable) afin d'empêcher un attaquant de cacher les traces de son attaque, et également garantir que les journaux sont examinés et surveillés et que des alertes sont en place pour détecter tout type d'événements ;
- ***Implémenter des systèmes de détection d'intrusion***, tant au niveau de l'hôte (« HIDS ») qu'au niveau de la couche réseau (« NIDS »). Ceux-ci peuvent utiliser plusieurs approches, notamment la détection basée sur les statistiques ou la détection basée sur le comportement, pour détecter des modèles inhabituels dans le comportement du système ou du réseau, ce qui peut indiquer qu'ils ont été compromis ou qu'une tentative d'exploitation est en cours ;
- ***Effectuer régulièrement un audit ou une analyse des vulnérabilités*** à l'aide d'un scanner de vulnérabilités qui analyse selon les « premiers principes » et est capable de découvrir des vulnérabilités même dans le code interne et personnalisé et là où aucune connaissance préalable d'une telle vulnérabilité n'existe ;
- Lorsque l'attaque est naissante ou en cours, ***assurer la suppression de l'accès pour maintenir l'attaquant hors du système ou du réseau***. Cette mesure est souvent appliquée au début, alors que la vulnérabilité est encore mal comprise, en supprimant simplement et entièrement la connectivité réseau de ce système ;
- ***Réaliser une « forensic investigation »*** robuste pour garantir que la vulnérabilité a été comprise ;
- ***Corriger la faille ou la faiblesse sous-jacente***, et souvent restaurer à un point antérieur à l'aide de systèmes de sauvegarde et de plans de reprise après sinistre.

5. En conclusion

"La science a la chance et la modestie de savoir qu'elle est dans le provisoire, de déplacer les frontières de l'inconnu et d'avancer." Marc Augé / Le Monde de l'éducation.

En bref, les attaques zéro-day sont parmi les menaces les plus insidieuses et difficiles à contrer dans le monde de la cybersécurité. Leur caractéristique la plus effrayante est le manque de préparation, car les vulnérabilités zéro-day sont inconnues et non corrigées au moment de leur utilisation. Cependant, en utilisant des solutions de sécurité avancées, en maintenant à jour les logiciels et en respectant les meilleures pratiques en matière de cybersécurité, on peut réduire considérablement les risques liés à l'exploitation de ces vulnérabilités.
