

## QU'EST-CE QUE LA GESTION DES CORRECTIFS ?

La gestion des correctifs, ou *patch management* en anglais, consiste à industrialiser les processus de détection, d'analyse et de déploiement des mises à jour des logiciels.

## POURQUOI EST-CE ESSENTIEL ?

- Corriger les bugs logiciels
- Supprimer les vulnérabilités exploitables pour les attaquants
- Profiter des nouvelles fonctionnalités de sécurité

## COMPRENDRE UNE VULNERABILITE

- Une vulnérabilité est identifiée par un **numéro CVE** (*Common Vulnerabilities and Exposures*)
- Sa criticité est quantifiée par un **score CVSS** (*Common Vulnerability Scoring System*) allant de **1 à 10**, le niveau le plus critique
- Une vulnérabilité non connue du public est qualifiée de **zero-day**

## MICROSOFT WINDOWS

### La gestion des composants Microsoft :

- **MBSA (Microsoft Baseline Security Analyzer)**

MBSA est l'outil recommandé pour analyser localement, comme à distance, la tenue à jour des composants Microsoft. Le rapport généré par l'outil contient la liste des correctifs non appliqués, leur niveau de criticité et les liens vers leur documentation.

- **Windows Update et WSUS (Windows Server Update Services)**

Windows Update est le service permettant la mise à jour des clients Windows. Il récupère et installe les mises à jour automatiquement auprès d'un serveur de référence Windows externe ou un serveur WSUS interne. Ce système permet aux administrateurs de s'assurer que seuls les correctifs testés et validés soient déployés l'organisation.

### La gestion des logiciels tiers :

Il n'existe pas pour cela de solution centralisée non propriétaire pour la mise à jour des logiciels non développé par Microsoft, ou *logiciels tiers*. On compte toutefois des outils natifs Microsoft:

- **SCUP (System Center Updates Publisher) & SCCM**

L'application SCUP gère un catalogue de mises à jour de logiciels tiers. Le déploiement est réalisable grâce à WSUS ou à l'outil SCCM (System Center Configuration Manager). Ce dernier est néanmoins payant et peut s'avérer complexe à utiliser.

## DISTRIBUTIONS LINUX

La gestion des mises à jour du système et des logiciels tiers est centralisée dans le gestionnaire de paquet : **apt** pour *Debian/Ubuntu* et **dnf/yum** pour *Redhat*. Ces outils gèrent nativement des fonctionnalités de contrôle d'intégrité et d'authenticité des paquets avec le standard OpenPGP.

Les paquets sont stockés dans des dépôts entretenus par l'éditeur ou la communauté en charge du développement de la distribution. Des dépôts locaux peuvent aussi être déployés pour contrôler plus finement les mises à jour autorisées sur les réseaux locaux.

### Déploiement des correctifs :

- **Satellite (Redhat) :**

Ce logiciel propriétaire et payant est développé par l'éditeur. Il permet la gestion de l'ensemble des hôtes Redhat d'une organisation et permet un déploiement centralisé des correctifs

- **unattended-upgrades / apt-listchanges (Debian) :**

Les mises à jour de sécurité peuvent être automatisées avec les programmes **unattended-upgrades** et **apt-listchanges**. Utile en cas d'absence de mises à jour centralisées.

## LES BONNES PRATIQUES

### Général

- Réaliser un inventaire des systèmes et des logiciels installés
- Réduire au minimum le nombre de programmes installés sur le parc pour simplifier la gestion
- Utiliser uniquement des canaux sécurisés pour télécharger les mises à jour (HTTPS)
- Utiliser des dépôts propres à l'organisation pour contrôler les mises à jour à appliquer.
- S'inscrire à un service de suivi des vulnérabilités
- Planifier régulièrement le déploiement des correctifs pour éviter les déploiements massifs
- Réaliser et diffuser une politique d'application des correctifs

### Application Web

- Limiter le nombre de greffons utilisés pour les gestionnaires de contenu.
- En cas de vulnérabilités critiques (CVSS 9+), passer les services web non critiques en mode maintenance, le temps que les correctifs soient déployés.

### Serveur

- Réaliser des montées de version uniquement vers des versions stables et testées
- Mettre à jour lors des périodes de faible activité (nuit / week-end)

## GESTIONNAIRES DE CONTENUS

Les gestionnaires de contenus et les applications web sont des cibles privilégiées pour les attaquants qui peuvent aisément trouver des systèmes vulnérables sur Internet. Il est donc important d'appliquer les correctifs de sécurité dès qu'ils sont disponibles.

Voici une liste des sites de référence pour la sécurité des principaux gestionnaires de contenus du marché :

- **Wordpress**
  - <https://wordpress.org/news/category/security/>
- **Drupal**
  - <https://www.drupal.org/security>
- **Joomla**
  - <https://developer.joomla.org/security.html>
  - <https://vel.joomla.org/> (greffons)
- **SPIP**
  - <https://stats.spip.net/SPIP-core>

Les greffons (plug-ins) de ces gestionnaires de contenu sont également une grande source de vulnérabilités et doivent bénéficier d'une gestion identique des correctifs.

## EQUIPEMENT RESEAU / IMPRIMANTE

Les firmwares et systèmes d'exploitation des équipements sont plus rarement mis à jour et sont une cible privilégiée pour les attaquants. Chaque constructeur publie régulièrement des correctifs. Quelques liens à titre d'exemple :

- **CISCO** :
  - [https://tools.cisco.com/security/center/softwarechecker\\_x](https://tools.cisco.com/security/center/softwarechecker_x)
- **HPE** :
  - <https://www.hpe.com/us/en/services/security-vulnerability.html>
- **DELL** :
  - <http://www.dell.com/support/home/fr/fr/frbsdt1?app=drivers>

## SUIVI DES VULNERABILITES

- <https://www.cert.ssi.gouv.fr/alerte/actives/>
- <https://cyberveille-sante.gouv.fr/>
- <https://nvd.nist.gov/>