

## Résumé

Ce document traite des patches de sécurité dont l'application doit permettre l'amélioration de la sécurité des logiciels présentant des failles caractéristiques. Sont décrits dans ce document les

principes d'application et de fonctionnement d'un patch, en tant que mesure préventive, ainsi que les menaces qu'il permet de contrer.

## Table des matières

- 1 C'est quoi ? →
- 2 Qui est concerné ? →
- 3 Comment cela fonctionne-t-il ? →
- 4 Pourquoi se protéger ? →
- 5 Comment se protéger ? →



## 1 C'est quoi ?

**Un patch est une mise à jour, sous forme de fichier ou logiciel, visant à corriger les failles de sécurité d'un système d'exploitation ou logiciel.**

Dans certains cas, un patch ne va pas, uniquement corriger la faille. En effet, il peut également ajouter de nouvelles fonctionnalités au logiciel informatique ou au système d'exploitation.

Les constructeurs mettent souvent un patch à disposition en téléchargement afin de répondre à des failles de sécurité éventuelles. À l'origine, les failles sont détectées, soit par les

testeurs et développeurs du constructeur, soit signalées par des utilisateurs externes.

## 2 Qui est concerné ?

Tous les citoyens, PME et administrations confondus, utilisant des outils relatifs aux Nouvelles Technologies de l'Information et de la Communication (N.T.I.C.).

## 3 Comment cela fonctionne ?

L'accroissement des fonctionnalités et possibilités offertes par les différents logiciels augmente la probabilité de contenir des failles de sécurité.

Ces failles peuvent dans certains cas être utilisées et exploitées à des fins malicieuses afin d'obtenir un accès non-autorisé sur la machine utilisant le logiciel défectueux.

Le cycle de vie d'un patch commence dans la majorité des cas par la notification de la faille par le constructeur du logiciel,

voire directement par une annonce publique. Dans des cas limités, et en fonction de certaines lois et réglementations nationales, l'annonce publique sans autorisation de la part du constructeur peut être considérée comme illicite.

A partir de cet instant et dans un laps de temps arbitraire, le constructeur de logiciel valide l'existence de la faille par une annonce ou la publication d'un bulletin de sécurité. Dans la plupart des cas, cette annonce est accompagnée simultanément de la mise à disposition d'un correctif (patch) permettant de contrer la faille existante.

→ suite

En fonction du niveau de maturité du constructeur, chaque patch devrait être accompagné d'une notice d'information ayant les caractéristiques suivantes :

- Identifiant unique incluant les notions de date et version du patch.
- Informations sur la faille de sécurité.

- Systèmes et logiciels affectés.
- Explications sur la mise en œuvre du patch.
- Informations de contact.
- Impacts potentiels ou tout autre type d'information importante à prendre en compte.

## 4

### Pourquoi se protéger ?

L'application de patches permet de contrer principalement les menaces suivantes :

- **Attaques** (Consultez la fiche : « Attaques »).
- **Vers/Virus** (Consultez la fiche : « Vers/Virus »).
- **Chevaux de Troie** (Consultez la fiche : « Chevaux de Troie »).

Voici un extrait d'un bulletin d'information relatif à une vulnérabilité et contenant les indications relatives au patch et aux versions disponibles :

Information on how to disable DCOM is available in Microsoft Knowledge Base Article [825256](#).

Notes For Windows 2000, the methods described above will only work on systems running Service Pack 4 or later. For Windows XP, the methods described above will only work on systems running Service Pack 2 or later. For Windows Server 2003, the methods described above will only work on systems running Service Pack 1 or later.

**Patch availability**

**Download locations for this patch**

- [Windows NT 4.0](#)
- [Windows NT 4.0 Terminal Server Edition](#)
- [Windows 2000](#)
- [Windows XP 32-bit Edition](#)
- [Windows XP 64-bit Edition](#)
- [Windows Server 2003 32-bit Edition](#)
- [Windows Server 2003 64-bit Edition](#)

**Additional information about this patch**

**Installation platforms:**

- The Windows NT 4.0 patch can be installed on systems running [Service Pack 4a](#).
- The Windows NT 4.0 Terminal Server Edition patch can be installed on systems running [Service Pack 4a](#).

## 5

### Comment se protéger ?

Avant d'installer un patch, il faut toujours considérer :

- Si vous êtes concerné par le patch et le cas échéant que vous téléchargez la version correspondante à votre environnement.
- Si le patch vous permet d'acquérir un niveau de sécurité supplémentaire par rapport à d'éventuelles contre-mesures déjà existantes tel que des anti-virus, firewalls ou autres.

- Dans certains cas, et surtout pour les entreprises, un patch peut lui-même créer des problèmes de disponibilité ou d'instabilité dans le système d'information et de communication. Il est par conséquent recommandé dans la mesure du possible de valider le patch en environnement de test avant de l'appliquer à l'environnement de production.