

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Acquisition des correctifs

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004>

Gestion du document

Référence	CERTA-2001-INF-004
Titre	Acquisition des correctifs
Date de la première version	04 octobre 2001
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Parmi les questions fréquemment posées au CERTA figure une inquiétude légitime concernant la confiance à accorder dans les correctifs à appliquer pour contrer une vulnérabilité. Cette inquiétude regroupe un ensemble de questions plus ou moins corrélées :

- 1° le remède n'est-il pas plus dangereux que le mal ? en d'autres termes : les correctifs à appliquer en catastrophe ne comportent-ils pas de vulnérabilités ?
- 2° est-ce bien prudent de recommander de télécharger des correctifs sur des serveurs connectés au réseau Internet ?

2 Les correctifs sont ils sûrs ?

Dès lors que l'on a obtenu par un canal sûr, les correctifs de la part de l'éditeur, la confiance dans le correctif se ramène à la confiance que l'on peut avoir dans l'éditeur.

Il n'y a aucune raison objective de soupçonner que les correctifs apporteront plus ou moins de fonctions cachées que le système d'exploitation ou l'application qu'ils corrigent. Vous pouvez vous forger une opinion sur le degré de sécurité apporté par un logiciel au regard de vos besoins de sécurité en demandant une évaluation du produit.

Indépendamment de toute suspicion que l'on pourrait éprouver à l'égard de tel ou tel éditeur de logiciel, il convient de se rappeler qu'un correctif est souvent un logiciel (c'est plus rarement de la documentation ou des données de configuration). Or l'état de l'art en matière de développement fait qu'on ne sait pas faire du logiciel sans défaut (même en appliquant des méthodes de développement basées sur une pratique mûre du génie logiciel, on parvient à abaisser le taux de défauts à une fourchette comprise entre 0,1 et 1 défaut par millier de lignes de code, ce qui est considéré comme un exploit en matière de qualité).

Les personnes qui développent des correctifs travaillent bien souvent avec un objectif très serré. Il s'agit d'une course entre eux et les pirates. En effet, dans le but d'inciter les éditeurs à corriger rapidement leurs logiciels, il existe des forums où les défauts sont mis sur la place publique. Il arrive que pour prouver la nocivité de la vulnérabilité, quelqu'un publie un programme qui l'exploite pour permettre par exemple d'acquérir des privilèges. Ces forums, y compris les plus sérieux, disposent d'une politique de divulgation qui, pour simplifier, pose un ultimatum aux éditeurs : « vous avez 45 jours pour publier votre correctif. Dans tous les cas nous publierons la vulnérabilité passé ce délai. Votre réputation est en jeu. » Il n'y a pas de consensus sur le bien fondé de cette politique de divulgation, certains pensent qu'il serait préférable de cacher la vulnérabilité avant qu'elle ne soit corrigée, la majorité des spécialistes pensent qu'il est illusoire de cacher la vulnérabilité ; la divulgation est l'aiguillon qui pousse l'éditeur à corriger son produit.

Cette pression sur les développeurs peut dans certains cas ne pas les placer dans les conditions les meilleures pour un développement sûr. Ainsi certains correctifs font l'objet de plusieurs versions ce qui aurait tendance à prouver la difficulté d'appréhender complètement un problème du premier coup.

Dans tous les cas, les correctifs peuvent entraîner des effets de bord. Un effet souvent constaté est le changement des éléments de l'interface homme-machine qui ne sont plus rédigés en français. D'autre part, certains correctifs récents s'appuient sur d'anciens composants logiciels (bibliothèques de fonctions partagées par exemple), réintroduisant ainsi une vulnérabilité que d'autres correctifs avaient entre temps supprimée.

3 Le téléchargement des correctifs est-il fiable ?

Non.

Les protocoles de l'Internet généralement utilisés pour accéder aux correctifs en ligne (FTP, HTTP) ne sont pas fiables. En effet, il est possible de détourner le DNS pour faire miroiter un faux site de téléchargement de correctifs. Il existe des outils servant à la sensibilisation au risque informatique qui font cela très bien.

Rien donc ne prouve que vous obtenez le correctif de la part de l'éditeur, à moins que celui ait mis en œuvre des procédés cryptographiques qui permettent d'authentifier les serveurs (SSL) et d'authentifier les fichiers (signature PGP ou GPG en général). Ces deux techniques ne sont pas exclusives l'une de l'autre. On peut aussi obtenir par un canal non sûr les fichiers de correctifs et par un canal sûr les condensés MD5 de ces fichiers.

Cependant ces techniques cryptographiques pour être efficaces doivent faire l'objet d'une attention particulière. On peut citer deux cas où des éléments cryptographiques ont été compromis. Le premier cas, le plus célèbre est celui d'un faux certificat SSL au nom d'un grand éditeur de logiciel signé par une autorité de certification non moins célèbre ; l'autre cas est celui d'un serveur compromis chez un autre grand éditeur, l'obligeant à révoquer certaines de ses clés PGP. Par ailleurs la confiance dans le protocole SSL, nécessite une compréhension des mécanismes sous-jacents.

Vous ne pourrez avoir confiance dans le mécanisme de téléchargement que lorsque vous êtes en relation avec un éditeur qui applique une signature des fichiers que vous pouvez vérifier parce que la clef de signature est sur un cédérom d'installation, par exemple (ou tout autre canal sûr de distribution de leurs clés), et que les procédures de gestion, par l'éditeur, de ses clés secrètes vous semblent sérieuses.

4 Le CERTA ne pourrait-il pas offrir un serveur de correctifs sûr ?

Non.

La première raison est qu'il appartient à l'éditeur du logiciel que vous avez choisi d'offrir un service de maintenance à la hauteur de ce que vous attendez. Cela peut constituer un critère de choix important dans l'acquisition d'un logiciel.

Le CERTA est confronté au même problème que chaque administrateur. S'il doit acquérir le correctif en ligne, il est soumis aux mêmes aléas.

La seconde raison est liée à la *propriété intellectuelle*. Les éditeurs assimilent souvent à de la contrefaçon quiconque prétend proposer leur logiciel, voire leurs avis de vulnérabilité recopiés *verbatim* sur un serveur WEB.

En revanche le CERTA a déjà et pourra être amené à diffuser des logiciels qu'il a écrit ou modifié lui-même.

5 Pourquoi dois-je appliquer un correctif s'il n'est pas sûr ?

C'est une question extrêmement pertinente.

La réponse n'est pas aisée et s'apprécie au regard de votre politique de sécurité. Toutefois la problématique peut se résumer en : « dois-je prendre le *risque* d'être compromis, intentionnellement ou non par mon fournisseur de logiciel, pour échapper à la *certitude* d'être compromis par un virus ou un pirate ? ».

Il semble que la réponse se ramène au choix suivant :

- il s'agit de lutter contre un nouveau logiciel malveillant qui exploite d'anciennes vulnérabilités dont les correctifs ont été publiés de longue date. Vous avez acquis ces correctifs par la maintenance selon un processus que vous avez validé lors de l'acquisition du logiciel vulnérable. Dans ce cas vous avez confiance dans les correctifs (ni plus ni moins que dans le logiciel original). Vous pouvez appliquer les correctifs comme vous le faites d'habitude.
- il s'agit de lutter contre une vulnérabilité récente très agressive ou dont les conséquences peuvent être graves pour l'organisation (fuite d'information, perte d'image de marque, matériel rendu inutilisable, ...). Il y a donc une certaine pression apportée par le contexte qui équilibre le soucis de ne pas être victime d'un correctif mal écrit ou compromis. Rien ne vous est imposé, l'alternative est donc :

1° vous estimez que le risque apporté par la vulnérabilité est plus grand que le risque d'avoir une porte dérobée ou un système bogué. Vous pouvez télécharger le correctif en gardant à l'esprit les risques associés et prenant les mesures appropriées pour le réduire (vérification des signatures par exemples). Personne ne vous empêche de tester le correctif sur une machine dont l'importance est moindre pour évaluer les éventuels effets de bord qui pourraient apparaître dans votre contexte d'utilisation.

2° vous estimez que le risque d'avoir un produit rendu instable par l'application d'un correctif dont vous ne savez pas à quel point il a été développé à la hâte est plus grand que le risque d'avoir un système compromis. Ce type d'approche peut se comprendre quand on a un système de production pour lequel on demande une grande disponibilité.

Toutefois, certains vers récents étant très agressifs, une machine connectée à Internet peut subir plusieurs dizaines voire centaines de tentatives d'exploitation de vulnérabilité par jour. Si bien qu'en restant connecté (ou dans n'importe quelles conditions de promiscuité informatique, comme de fréquents échanges de disquettes par exemple) vous multipliez vos chances d'être compromis.

La compromission sera un moindre mal, puisque vous ne placez pas de données sensibles sur une machine connectée à Internet, n'est-ce pas ? D'autre part votre service juridique est prêt à traiter les plaintes qui pourraient survenir de tiers dont la machine serait agressée par la vôtre suite à une compromission utilisant la vulnérabilité pour laquelle vous ne souhaitez pas appliquer des correctifs acquis de façon non sûre.

Dans ce cas vous pouvez laisser la machine branchée en espérant que les correctifs soient sur le prochain cédérom de maintenance (ou tout canal qui vous semble suffisamment sûr).

3° vous estimez que le risque est plus grand d'attendre les correctifs ou de les télécharger, mais que néanmoins le service doit être rendu. Vous pouvez envisager de changer de logiciel pour prendre un autre qui vous semble plus sûr. La sûreté est une notion relative qui s'effiloche avec le temps. Il n'y a pas de solution miracle définitive. En outre il est risqué de changer une architecture validée.

4° vous estimez que le risque d'être compromis est plus grand que celui de ne plus offrir le service. Vous pouvez couper l'accès à Internet. De toutes les solutions évoquées ici, c'est souvent la moins populaire auprès des usagers.

5° ...

En conséquence le CERTA ne peut pas prendre la décision à votre place, dans la mesure où aucune des solutions n'est totalement satisfaisante et que la pondération des différents risques dépend de vos besoins. Le rôle d'un CERT est de vous avertir de l'agressivité de certains logiciels malveillants ou bien de vulnérabilités qui pourraient être exploitées et de signaler les correctifs qui, a priori, remettent en cause le moins possible vos choix d'architecture de sécurité.

Gestion détaillée du document

04 octobre 2001 version initiale.