

MARC BLANCHARD VIRUS DOCTEUR

[Appel à Réponse] Pour Marc Olanié Réseaux & Télécom du 12 Septembre 2007

En réponse à Marc Olanié sur son article sur la vulnérabilité de KAV et KIS 6 et 7 publiée sur rootkit.com , je voudrais apporter quelques explications.

Ce qu'il faut savoir sur cette vulnérabilité est **la grande difficulté avec laquelle on peut l'exploiter.**

Dans un premier temps, cette vulnérabilité ne peut fonctionner, que si et seulement si, Windows est ouvert !!! peu probable dans les versions XP/Vista!

A savoir qu'un partage réseau n'est pas suffisant. Il faut que l'administrateur du poste Windows permette non seulement un partage réseau, mais également le fait **qu'une personne extérieure puisse exécuter des programmes à distance!**

Chose qui, n'est évidemment pas autorisé par défaut lors des installations des OS Windows.

L'impossible étant possible, pour que cette attaque puisse fonctionner, il faudrait que le poste soit infecté par une backdoor, que cette backdoor ouvre un port TCPIP, qu'elle puisse permettre d'exécuter un programme, que ce programme soit poussé par le créateur, puis ensuite que le créateur puisse accéder à la machine pour son lancement, pour qu'ensuite, de nombreux écrans bleus apparaissent, pour qu'au final, l'utilisateur appuie sur son interrupteur d'arrêt de la machine pour la redemarrer.

Cela fait beaucoup de choses pour un écran bleu ou l'extinction du PCpas gloup!!!!

Les utilisateurs possédant Kaspersky, mettent à jour leurs bases antivirus en moyenne toutes les heures..ou moins, si ils ont choisi de mettre la mise à jour des bases en automatique.

Actuellement (voir les stats des fréquences de mises à jours de nos viruslabs) , on peut constater que depuis plus d'un mois maintenant, environ toutes les 39 minutes, de nouvelles bases sont disponibles au téléchargement. Téléchargement, qui, par défaut dans KAV/KIS 6 et 7, sont automatiques.

Les probabilités d'infections via une backdoor, puis la réception d'un malware qui permettra l'exécution de l'exploit, se trouvent minimisées.

D'autre part, la PDM (le module proactive défense du moteur) permet une exécution et une

vérification dans une sandbox heuristique des codes ne reagissant pas aux signatures. Cette PDM permet notamment d'analyser les intégrités du système (toute exécution est contrôlée, mais aussi une analyse de l'activité de la registre, des processus, des installations et exécutions cachées).

Vous me direz : c'est là que l'exploit intervient !!

Je vous répondrai, oui, mais comment pourrait-il se copier, s'exécuter si il est bloqué par les analyses des AVBases ou de la proactive défense?

De même, étant donné que cet exploit ne peut se lancer qu'en effectuant un éventuel contrôle total à distance de la machine, il est difficilement probable que cet exploit s'active dans le monde à petite, moyenne ou grande échelle.....

Bref, suite au collègue que j'ai eu avec notre équipe de développeurs gérant les vulnérabilités, on peut dire que cette vulnérabilité est classée au niveau BAS.

Nous travaillons actuellement dessus et la mise à jour de KLIF.SYS sera effectuée de façon automatique sur KAV/KIS.

Donc pas de panique face à cet exploit, qui, je vois, commence à faire couler de l'encre !

Commentaires

2007-09-20 18:16:01 - Jean 32

Bonjour Marc Blanchard,

Si j'ai bien compris les màj des bases antivirales, chaque 39 minutes, il serait préférable de laisser en automatique, qui est par défaut, à la place de chaque heure, qui est ma seule modification que je fais depuis KIS 6 ?

Avec cette modif, je "perds" 21 minutes de réaction de KIS 7.0.0.125, me semble-t-il. Est-ce important ?

Me faudrait-il remettre en automatique ? Si tel est le cas, une annonce au début du forum de KIS par le Lab- ne serait-elle pas judicieuse ?

Merci encore pour toutes ces infos, avec mes amitiés,

Jean 32

2007-10-04 16:45:10 - Jean 32

Bonjour Marc Blanchard, (un copier/coller du 20 septembre 2007) absent ce jour jusqu'au 12-10-07, serait-il possible d'avoir votre avis sur ce sujet de màj automatique ou chaque heure ?

Si j'ai bien compris les màj des bases antivirales, chaque 39 minutes, il serait préférable de laisser en automatique, qui est par défaut, à la place de chaque heure, qui est ma seule modification que je fais depuis KIS 6 ?

Avec cette modif, je "perds" 21 minutes de réaction de KIS 7.0.0.125, me semble-t-il. Est-ce important ?

Me faudrait-il remettre en automatique ? Si tel est le cas, une annonce au début du forum de KIS par le Lab- ne serait-elle pas judicieuse ?

Merci encore pour toutes ces infos, avec mes amitiés,

2007-10-04 17:01:43 - Marc Blanchard [Virus Docteur] - marc.blanchard@fr.kaspersky.com

Le fait de mettre en automatique KIS/KAV permet d'avoir en quasi-temps réel les mises à jours des bases. Pour info, regardez les stats des mises à jours des bases sur ce blog dans la catégorie Statistiques en ligne. Cela permet également, en cas de propagation importante, de laisser le VirusLab de Kaspersky, de forcer votre antivirus à se mettre à jour, et ainsi diminuer les probabilités de recevoir le virus en cours de propagation.

Copyright : Blanchard [Virus Docteur] Marc - 2007-09-14 12:43:54
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>