

# Retour sur la vulnérabilité MS08-001

Certaines failles de sécurité défilent la chronique et c'est le cas par exemple de la première cuvée Microsoft 2008 [1]. Les deux vulnérabilités corrigées touchent directement le noyau Windows dans sa gestion des protocoles TCP/IP. L'une d'entre elles [2] affecte les principaux systèmes Windows (XP, 2003 et Vista) dans leur configuration par défaut (pour XP et Vista). Elle est située dans les portions de code traitant les structures TCP/IP mémorisant l'état des requêtes IGMPv3 et MLDv2, ce type de requêtes étant utilisé pour la gestion du trafic multicast SSM (*Source-Specific Multicast*) en IPv4 (IGMPv3) et en IPv6 (MLDv2). L'exploitation de cette vulnérabilité permet l'exécution de code à distance, sans authentification préalable et dans le contexte noyau, en envoyant des paquets IGMPv3 pour Windows XP et MLDv2 pour Windows Vista. Quand on sait que par défaut, IGMPv3 et MLDv2 traversent les pare-feu des Windows XP SP2 et Vista, on comprend vite le danger d'une telle faille. Comme à l'accoutumée, de nombreux chercheurs ont étudié [3] le correctif pour analyser les portions de codes corrigées. L'exploitation de cette faille, au delà du déni de service, était jugée *peu probable* par Microsoft [4] mais Kostya Kortchinsky a réussi à l'exploiter correctement, du moins sur des Windows XP [5]. La fiabilité est selon lui de 90% si tous les paquets arrivent dans l'ordre à la cible. L'animation Flash publiée sur le site d'Immunity Inc. [6] montre la compromission simultanée de deux Windows XP.. merci le multicast ! L'exploitation de la faille sur Windows Vista via le protocole MLDv2 (IPv6) apparaît possible mais plus complexe car elle nécessite l'envoi d'environ

quatre fois plus de paquets, ce qui influe négativement sur le taux de succès [7].

Cette faille est la première exploitable à distance sur un Windows XP SP2 avec un pare-feu configuré par défaut, le tout en espace noyau. La présence de cette vulnérabilité à un niveau aussi bas la rend difficilement détectable par la plupart des solutions de protection des postes de travail du marché (HIPS, etc.). En effet, ces dernières travaillent souvent à un niveau plus élevé, comme le rappellent les deux chercheurs ayant rapporté ces vulnérabilités à Microsoft [8]. Le code d'exploitation n'est pas public et apparaît complexe à développer ce qui évitera peut être une vague de vers comme on

a pu en voir dans le passé, au moins à court terme... De telles possibilités de compromissions massives risquent de pousser de nombreuses personnes malveillantes à travailler sur l'exploitation de cette vulnérabilité à des fins pécuniaires (installation de *backdoors*, *keyloggers* ou autres).

L'exploitation distante de cette vulnérabilité dans la pile réseau va donc ici bien plus loin qu'un déni de service. Il est aujourd'hui possible de compromettre de nombreuses machines à distance en exploitant une vulnérabilité noyau et en exécutant du code arbitraire... même si la création de tels codes d'exploitation n'est pas à la portée de tout le monde.



## Guillaume Lehembre

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants - <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et s'intéresse de près à des sujets comme la sécurité des réseaux sans fils et la voix sur IP. Il a réalisé des interventions publiques sur ces sujets et a publié plusieurs articles, dont un article dans le numéro 14 de *hakin9* intitulé Sécurité Wi-Fi – WEP, WPA et WPA2. Il rédige un éditorial mensuel dans *Hakin9* depuis Janvier 2007. Guillaume peut être contacté à l'adresse suivante : [Guillaume.Lehembre@hsc.fr](mailto:Guillaume.Lehembre@hsc.fr)

## Références

- [1] <http://www.microsoft.com/france/technet/security/bulletin/ms08-001.msp>
- [2] <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0069>
- [3] <http://www.zynamics.com/files/ms08001.swf>
- [4] <http://blogs.technet.com/swi/archive/2008/01/08/ms08-001-part-3-the-case-of-the-igmp-network-critical.aspx>
- [5] <http://expertmiami.blogspot.com/2008/01/cetaut-pas-gagne.html>
- [6] [http://www.immunityinc.com/documentation/ms08\\_001.html](http://www.immunityinc.com/documentation/ms08_001.html)
- [7] <http://expertmiami.blogspot.com/2008/02/et-vista-dans-tout-ca.html>
- [8] <http://blogs.iss.net/archive/howtoprotectMS08-001.html>