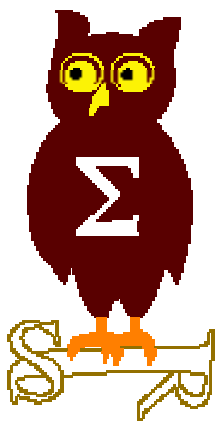
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 7 février 2005



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/7)

EdelWeb

- **Avis de sécurité Microsoft depuis le 13 décembre 2004**
  - **MS04-041 vulnérabilité Wordpad**
    - **Affecte : Windows NT4, 2000, XP, 2003**
    - **Exploit : double "buffer overflow" dans le convertisseur Word 6.0**
      - **CAN-2004-0571 et CAN-2004-0901**
      - **Avez-vous pensé à filtrer les .WRI ?**
    - **Crédit : Greg Jones (KPMG UK), "Lord Yup" (iDefense)**
  - **MS04-042 "buffer overflow" dans DHCP**
    - **Affecte : Windows NT4 Server**
    - **Exploit : double "buffer overflow"**
      - **Requête (CAN-2004-0900) et journalisation (CAN-2004-0899)**
    - **Crédit : Kostya Kortchinsky**
  - **MS04-043 vulnérabilité HyperTerminal**
    - **Affecte : Windows NT4, 2000, XP, 2003**
    - **Exploit : "heap overflow" exploitable via un ".ht" ou une URL telnet://**
      - **CAN-2004-0568**
      - **Exploitable également sous XP SP2 car un pointeur de fonction est écrasé**
    - **Crédit : Brett Moore**

Dernières vulnérabilités
Avis Microsoft (2/7)

EdelWeb

- MS04-044 élévation(s) de privilèges locale(s)
  - Affecte :
    - 1/ Windows NT4, 2000, XP, 2003
    - 2/ Windows 2000, XP, 2003
  - Exploit :
    - 1/ CAN-2004-0893 : "heap overflow" via LPC (détails publiés)
    - 2/ CAN-2004-0894 : abus des "identity tokens" pour usurper l'identité de n'importe quel utilisateur connecté au système (détails publiés)
  - Crédit : Cesar Cerrudo / AppSec Inc.

- MS04-045 vulnérabilités WINS
  - Affecte : Windows NT4 Server, 2000 Server, 2003
  - Exploit : "buffer overflow" (CAN-2004-0567) et passage de pointeur (CAN-2004-1080)
    - Disponible dans Metasploit 2.3
    - Ver « WINSER » (installe le cheval de Troie « HZDOOR »)
      - http://www.unixwiz.net/research/winser-a.html
  - Crédit : Kostya Kortchinsky

Dernières vulnérabilités
Avis Microsoft (3/7)

EdelWeb

- **Re-release**
  - **MS04-028 bogue GDI+**
    - **Nouveau logiciels impactés : .NET Framework 1.0 et 1.1, FoxPro 8.0 et 9.0, Messenger 5.1**

- **Avis de sécurité Microsoft depuis le 10 janvier 2004**
  - **MS05-001 Vulnérabilité(s) dans l'aide HTML**
    - **Affecte : Windows 2000, XP, 2003**
      - **Windows NT4 peut être impacté si IE 6 est installé**
    - **Exploit : exécution de script dans la zone poste de travail via HHCTRL.OCX (complexe)**
      - **CAN-2004-1043**
      - **Alertes**
        - **http://www.securityfocus.com/bid/11467**
        - **http://secunia.com/advisories/12889**
      - **Analyse**
        - **http://freehost07.websamba.com/greyhats/sp2rc-analysis.htm**

Dernières vulnérabilités
Avis Microsoft (4/7)

EdelWeb

- PoC
  - http://freehost07.websamba.com/greyhats/sp2rc.htm
  - http://malware.com/noceegar.html
  - http://www.michaelevanchik.com/security/microsoft/ie/xss/index.html
  - http://www.michaelevanchik.com/security/microsoft/ie/xss/writehta.txt
- Propagation dans la nature du cheval de Troie "Phel"

– Crédit : Michael Evanchik, Paul, et d'autres

- Variante également patchée
  - PoC :
    - http://www.freewebs.com/shreddersub7/htm.htm
    - http://www.freewebs.com/shreddersub7/expl-discuss.htm
  - Crédit : ShredderSub7
  - Notes :
    - "hhctrl.ocx" ne serait pas installé avec Windows XP SP1
    - Mais serait installé par défaut dans Windows XP SP2
    - Il n'est pas exclu que d'autres variantes puissent fonctionner !
      - http://www.gecadnet.ro/windows/?AID=1381

Dernières vulnérabilités
Avis Microsoft (5/7)

EdelWeb

- **MS05-002 Vulnérabilités multiples dans le traitement des fichiers images**
  - **Affecte : Windows NT4, 2000, XP (sauf SP2), 2003**
  - **Exploit :**
  - **1/ CAN-2004-1049**
    - **"Heap overflow" dans USER32!LoadImage()**
      - **Exécution de code via un fichier BMP / CUR / ANI / ICO malformé**
    - **PoC publié**
    - **Patch non officiel publié avant le correctif officiel**
      - **http://sec-labs.hack.pl/patch/ico_patch2.zip**
  - **2/ CAN-2004-1305**
    - **Déni de service Windows via un fichier ANI malformé**
    - **PoC : nombre de trames = 0 …**
  - **Crédit :**
    - **1/ eEye**
      - **http://www.eeye.com/html/research/advisories/AD20050111.html**
    - **2/ Sylvain Bruyere**

Dernières vulnérabilités
Avis Microsoft (6/7)

- "0-day" initialement publiés par FlashSky / XFocus
  - http://www.xfocus.net/flashsky/icoExp/index.html
- Autre faille (non patchée celle-ci) :
  - "Heap overflow" et "integer overflow" dans "winhlp32.exe"
    - Affecte : toutes les versions de Windows (y compris SP2)
    - Exploit : fichier .HLP malformé
- MS05-003 Vulnérabilité dans le service d'indexation
  - Affecte : Windows 2000, XP (sauf SP2), 2003
  - Exploit :
    - CAN-2004-0897
    - "Buffer overflow" exploitable à travers IIS ou un accès distant au service d'indexation via SMB (requière une authentification)
  - Crédit : N/A

Dernières vulnérabilités
Avis Microsoft (7/7)

EdelWeb

- http://www.microsoft.com/technet/security/bulletin/advance.mspx

- Le mois de février s'annonce chaud
  - 9 Microsoft Security Bulletins affecting Microsoft Windows. The greatest aggregate, maximum severity rating for these security updates is Critical. Some of these updates will require a restart.
  - 1 Microsoft Security Bulletin affecting Microsoft SharePoint Services and Office. The greatest aggregate, maximum severity rating for this security bulletin is Moderate. These updates may or may not require a restart.
  - 1 Microsoft Security Bulletin affecting Microsoft .NET Framework. The greatest aggregate, maximum severity rating for this security bulletin is Important. This update will require a restart.
  - 1 Microsoft Security Bulletin affecting Microsoft Office and Visual Studio. The greatest aggregate, maximum severity rating for this security bulletin is Critical. These updates will require a restart.
  - 1 Microsoft Security Bulletin affecting Microsoft Windows, Windows Media Player, and MSN Messenger. The greatest aggregate, maximum severity rating for these security updates is Critical. These updates will require a restart.

Dernières vulnérabilités
Infos Microsoft (1/3)

EdelWeb

- **Windows 2003 SP1 RC1**
  - **http://www.microsoft.com/windowsserver2003/downloads/servicepacks/sp1/default.mspx**
  - **De nombreuses nouveautés (un "XP SP2 like")**
  - **316 Mo …**
- **"Update Rollup" pour Windows 2000**
  - **Prévu mi-2005**
  - **http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/rollup.asp**
  - **Rappel : fin du support "standard" à partir du 30 juin**
    - **http://www.vnunet.com/news/1160791**
- **Programme "Microsoft Genuine"**
  - **Vérification du numéro de licence Windows avant tout téléchargement**
  - **A partir du 7 février : obligatoire pour Norvège, Chine, République Tchèque**

Dernières vulnérabilités
Infos Microsoft (2/3)

EdelWeb

- Microsoft rachète l'anti-spyware de Giant Company
  - http://www.giantcompany.com/
  - http://www.microsoft.com/athome/security/spyware/default.mspx
  - La Beta 1 du nouveau produit est disponible
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&DisplayLang=en
- Microsoft abandonne Passport
  - Défection de eBay et Monster
    - http://seattletimes.nwsource.com/html/businesstechnology/2002136272_passport31.html
  - Des alternatives …
    - Liberty Alliance
    - https://sxip.org/
    - http://www.myuid.com/

Dernières vulnérabilités
Infos Microsoft (3/3)

EdelWeb

- **Microsoft Security Risk Self Assessment**
  - Un outil d'auto-évaluation des risques de sécurité
  - http://go.microsoft.com/?linkid=1951173
- **Microsoft EPAL**
  - Elevated Privileges Application Launcher
  - Permet d'exécuter des applications (enregistrées dans AD) avec un niveau de privilèges "administrateur"
  - http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/epal.mspx
- **Microsoft sortira son propre antivirus en 2005**
  - http://www.zdnet.fr/actualites/telecoms/0,39040748,39163407,00.htm
  - Le produit est une fusion de :
    - Gecad Software (base de signatures)
    - Pelican Software (analyse comportementale).
- **Windows XP Pro 64 bits passe en RC1**

Dernières vulnérabilités XP SP2 (1/1)

EdelWeb

- Contournement du "popup blocker"
  - Affecte : IE 6 SP2
  - Exploit : http://www.malware.com/flopup.html
  - Crédit : Liu Die Yu
- Microsoft publie discrètement un correctif critique pour une faille ICF
  - Lors d'une migration SP1 vers SP2, Internet peut être considéré comme une zone de confiance dans ICF
  - Références
    - http://www.pcwelt.de/know-how/extras/103039/
    - Réunion OSSIR du 11/10/04
  - Correctif :
    - http://support.microsoft.com/kb/886185
    - http://www.microsoft.com/downloads/details.aspx?familyid=da66a0ac-55ca-4591-b3e6-d78695899141&displaylang=en
- Contournement de la protection du "heap" sur XP SP2 ?
  - http://www.maxpatrol.com/defeating-xpsp2-heap-protection.pdf

Dernières vulnérabilités
Autres avis (1/6)

- **Le chiffrement Office est cassable**
  - Affecte : Office 2000, XP (autres non testés)
  - Exploit : http://www.securityfocus.com/bid/12223
  - Crédit : Hongjun Wu
    - http://eprint.iacr.org/2005/007.pdf
  - Encore un problème de réutilisation de flux RC4 ...

- **"Buffer overflow" dans Acrobat Reader**
  - Affecte :
    - Acrobat Reader <= 6.0.2 (Windows)
    - Acrobat Reader <= 5.0.9 (Linux)
  - Exploit :
    - "Buffer overflow" dans la fonction mailListIsPdf()
    - Problème dans la gestion des fichiers ".etd"
  - Crédit : Greg MacManus
  - Note : les mises à jour françaises tardent à être publiées !

Dernières vulnérabilités
Autres avis (2/6)

EdelWeb

- **Un bogue Google !**
  - **http://www.google.pl/search?q=allegro.hit.gemius.pl**
  - **allegro.hit.gemius.pl = 255.255.255.255**
  - **Résultat : SEGFAULT**
- **Sortie de HFNetChk 4.3**
  - **Nombreuses nouveautés**
    - **Ex. supporte Apache 1.3/2.0 et Winzip**
    - **Pour concurrencer WUS ?**
- **Attention à l'encodage RFC 2397 !**
  - **Des images ou des exécutables peuvent être inclus en Base64 dans le corps d'un email ou d'une page Web**
    - **Ex. <img src="…**
  - **Supporté par de nombreux clients (sauf IE !)**
  - **A rapprocher d'un "bogue" Outlook 2003 ?**
    - **http://www.securityfocus.com/bid/11446**
  - **Les produits de sécurité ne scannent pas (tous) ce type de contenu**

Dernières vulnérabilités
Autres avis (3/6)

- **Promouvoir un serveur NT4 en PDC sans réinstallation : UPromote**
  - **http://utools.com/UPromote.asp**
- **Les failles de PocketIE (la version Windows Mobile de IE)**
  - **http://www.airscanner.com/tests/ie_flaw/ie_attack.htm**
  - **Rien de dramatique, car les capacités de PocketIE sont très limitées (pas de IFRAME)**
- **Netcraft sort sa barre anti-phishing**
  - **http://news.netcraft.com/archives/2004/12/28/netcraft_antiphishing_toolbar_available_for_download.html**
- **Un étudiant condamné en France pour "phishing"**
  - **http://www.clubic.com/actualite-18344-premiere-condamnation-pour-phishing-en-france.html**
  - **12 clients du Crédit Lyonnais abusé**
  - **Préjudice 20 000 euros**
  - **1 an de prison avec sursis et 8 500 euros de dommages et intérêts**

Dernières vulnérabilités
Autres avis (4/6) - virus

EdelWeb

- Alerte sur Zafi.D, Bagle.AY, Sober.J chez plusieurs éditeurs
  - Propagation importante
- Des fichiers WMV infectés par Trj/WmvDownloader
  - Affecte : Windows Media Player 10 (Windows XP SP2)
  - http://www.pandasoftware.com/about/press/viewNews.aspx?noticia=5818
  - Utilisation du système de DRM pour installer du spyware (!)
- Tegam vs. Guillermito
  - Motif retenu : violation de l'article 335.2 du code de la propriété intellectuelle (désassemblage de l'antivirus)
  - Peine requise : 4 mois de prison avec sursis et 6000 euros d'amende
  - Jugement le 8 mars 2005

Dernières vulnérabilités
Autres avis (5/6) – bogues IE

EdelWeb

- Un site à surveiller
  - http://0daymon.org/monitor/
- "Directory Traversal" dans le client FTP d'IE
  - Affecte : IE 6 (sauf XP SP2)
  - Exploit : lorsque IE est utilisé comme client FTP, il est possible de lui passer des URLs malformées afin de fausser la destination du téléchargement
  - Source : 7a69ezine
- IE peut envoyer un mail via une URL ftp://…%0a%0d…
  - Bogue déjà plus ou moins connu
  - http://dsbl.org/testingground/IE-FTP-SMTP-link/
  - Source : 7a69ezine
- Cross-site loading : invocation de scripts locaux par une page distante
  - http://www.edup.tudelft.nl/~bjwever/advisory_ie_flaws.html.php

Dernières vulnérabilités
Autres avis (6/6) – bogues IE

- **Cross-site scripting via execScript()**
  - **Affecte : IE toutes versions (y compris XP SP2)**
  - **Exploit :**
    - **http://secunia.com/advisories/13482/**
    - **http://news.zdnet.co.uk/internet/security/0,39020375,39181466,00.htm**

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion
  - Lundi 7 mars 2005
- N'hésitez pas à proposer des sujets et des salles