Faille WMF

Présentation pour le groupe SUR (Sécurité Unix et Réseaux)
10/01/2006

Saâd Kadhi <saad.kadhi@hapsis.fr>

Agenda

- WMF : le format
- WMF : la faille
- Moyens de protection
- Enseignements
- Dernière Minute !
- Références, Remerciements

WMF : le format

(ou comment faire moins avec plus)

Images WMF

- WMF : Windows MetaFile
- Format de fichiers graphiques de type vectoriel
  - 16-bit, introduit par Microsoft Windows 3.0
  - peu utilisé en comparaison à JPEG, GIF, PNG...
- EMF : Enhanced MetaFile
  - version 32-bit “améliorée”

Principes

- WMF est proche en termes de conception et d'objectifs de PostScript
- Un fichier WMF est un ensemble d'appels à des fonctions
- Ces appels sont envoyés à GDI pour affichage
  - différent des formats plus classiques "tel pixel est de telle couleur"

GDI

- GDI (Graphics Device Interface) est la couche graphique de Microsoft Windows
- Un des trois sous-systèmes clés de cet OS
- Utilisé pour représenter des objets graphiques et les afficher sur des fenêtres, écrans, imprimantes...
- Se manifeste sous forme de DLL (gdi32.dll), exécutée avec des privilèges SYSTEM

Identification du format

- Plusieurs applications Windows reconnaissent un fichier WMF à l'aide d'un "magic byte" stocké dans son en-tête
  - Internet Explorer, Explorateur de fichiers, Google Desktop Search, Outlook, Lotus Notes, ...

Exécution de code

- Les appels stockés dans un fichier WMF permettent d'exécuter du code
- Certains de ces appels sont sensibles et ne devraient pas venir de sources non sûres
- Par exemple, des appels de type "escape" qui permettent d'envoyer des données spéciales directement au dispositif d'affichage

SETABORTPROC - 1

- SETABORTPROC est un de ces appels
- Il permet à une application de signaler à GDI qu'elle comporte une fonction de :
  - gestion d'erreurs au niveau du spouleur ou
  - de suppression de travaux d'impression

SETABORTPROC - 2

- SETABORTPROC a été rendu obsolète par l'introduction de Win32
  - mais le code pour le gérer est toujours présent ! (compatibilité descendante)
- Une des façons de l'utiliser consiste à passer par Microsoft Picture and Fax Viewer (shimgvw.dll)

WMF : la faille

(à compatibilité descendante, sécurité ..)

Faille

- Une faille a été découverte par un dénommé “noemailpls” le 27.12.2005
  - lorsqu’il a trouvé un fichier WMF malicieux sur un site Internet
- La faille se situe au niveau de l’appel SETABORTPROC de gdi32.dll

Conséquences

- Exécution de code arbitraire avec les privilèges SYSTEM
  - autant dire une compromission totale...
- ...aggravée par le nombre impressionnant de vecteurs
  - Internet Explorer, Explorateur de fichiers, Google Desktop Search et toute application cherchant à afficher une image WMF

Plates-formes touchées

- Toutes les versions de Microsoft Windows disponibles depuis 1990
  - ça fait combien de victimes potentielles ?
- Windows XP et antérieur sont les plus vulnérables
  - car offrant par défaut un moyen de gérer et de lire les fichiers WMF

Codes d'exploitation

- Les codes d'exploitation de cette faille se sont multiplié à vitesse grand V (Sophos en recensait plus de 200 au 04.01.2006)
- Certains sont apparus très très vite
  - comme celui intégré à Metasploit, dont la deuxième version est de grande qualité
  - ou SATILOLER.B, le troyen de vols d'identifiants bancaires

Catastrophe annoncée - 1

- Faille “découverte” le 27.12.2005 permettant d’exécuter du code arbitraire avec des privilèges très elevés
- Exploit déjà sur Internet, 200+ recensés après en 9 jours
  - Il y en a peut-être (certainement ?) d’autres qu’on ne voit pas

Catastrophe annoncée - 2

- Exécution possible de manière automatique (via Internet Explorer par exemple) et peu importe l'extension
- En pleine période de fêtes
  - effectif réduit dans les entreprises
  - circulation massive de cartes de voeux électroniques en début d'année

Et Unix/Linux dans tout ça ?

- Rebond, quand tu nous tiens
  - exploitants sous Windows accèdant à des serveurs de production critiques
- WINE vulnérable selon H D Moore du projet Metasploit
- D'autres émulateurs le sont peut-être aussi

Moyens de protection

(rustines ou armure russe ?)

Introduction

- 5 moyens de protection principaux ont été proposés
  - désactivation de DLL
  - filtrage de fichiers
  - logiciels anti-virus
  - correctif non officiel
  - correctif officiel

Désactivation de DLL - 1

- Cette solution consiste à désactiver la DLL shimgvw.dll

```
regsvr32 -u %windir%\system32\shimgvw.dll
```

- Cette DLL est utilisée par les codes d'exploitation (pas tous ?) pour passer l'appel SETABORTPROC à gdi32.dll
- Solution préconisée par l'éditeur
  - sans impact majeur sur le fonctionnement de Windows

Désactivation de DLL - 2

- Solution partielle
  - il peut y avoir d'autres moyens de passer l'appel causant la faille à la couche GDI
- Au mieux, une rustine
  - L'ISC (Internet Storm Center) a découvert des cas où des applications réactivaient la DLL en silence

Filtrage de fichiers

- Le filtrage de fichiers ne peut être efficace que
  - s'il est effectué sur l'en-tête des fichiers
  - s'il voit passer tous les fichiers (clés USB, connexions chiffrées, canaux couverts, ...)
- Autant dire que c'est loin d'être la panacée
  - mais Defense-In-Depth oblige, c'est recommandé

Logiciels anti-virus

- Les logiciels anti-virus sont une protection convenable une fois les codes d'exploitation "révélés" et décortiqués par les éditeurs
- Catch-up Game(tm)
  - 200+ codes d'exploitation "découverts" et ça augmente !
  - et les codes d'exploitation non découverts ?

Correctif non officiel - 1

- Le 01.01.2006, soit 3 jours après la découverte de la faille WMF, Ilfak Guilfanov propose un correctif
  - expert mondialement reconnu de la plate-forme Windows
  - créateur de IDA Pro
- Blocage de toutes les tentatives d'utiliser SETABORTPROC

Correctif non officiel - 2

- Ce correctif travaille uniquement en mémoire
  - DLL wmfhotfix.dll injectée en mémoire
- Aucune modification n'est effectuée au niveau de gdi32.dll ou de tout autre fichier Windows
- Il ne peut en aucun cas interférer avec un correctif officiel de Microsoft

Correctif non officiel - 3

- Très facile à désinstaller, il a été testé et fortement recommandé par l'ISC et F-Secure
- Protection totale contre la faille WMF...
- ... sauf si on arrive à "décharger" wmfhotfix.dll mais les tests n'ont pas confirmé cette hypothèse

Correctif officiel

- Après avoir annoncé son propre correctif pour le 10.01.2006, Microsoft le sort en avance le 05.01.2006 (aux alentours de 20h15 heure française)
  - de la pression dans l'air ?
- Il est fonctionnellement identique au correctif non officiel
  - sauf qu'il corrige directement la DLL (accès au code source oblige)

Correctif vs. correctif

- L'éditeur et certains "experts" sécurité se sont plus ou moins acharnés contre le correctif d'Ilfak
  - il causerait des effets secondaires (problèmes d'impression)
- Mais le correctif de Microsoft causerait les mêmes problèmes
- Rappelons que SETABORTPROC est obsolète. Les pilotes l'utilisant encore sont douteux

Nu ou protégé

- Le correctif d'Ilfak a été validé par des instances sécurité telles que l'ISC, F-Secure, et Sophos
  - code source disponible
- Mais il n'a pas été déployé dans beaucoup d'entreprises
  - "on va perdre le support Microsoft !!!"
  - question : Avez-vous déjà lu l'EULA de Windows ?

Enseignements

("Thinking the public exploit is the only one is plain stupid" - darkspyrit)

Enseignements - 1

- Les images ne sont pas des fichiers “sûrs”
- La monoculture est dangeureuse. Elle va à l’encontre du bon sens “sécurité”
- La compatibilité descendante peut être dangeureuse

Enseignements - 2

- La compatibilité descendante doit être limitée dans le temps
- Trop d'intelligence tue l'intelligence
- Les codes d'exploitation ciblés existent. Et ce sont les plus dangeureux
- Il est temps que les éditeurs logiciels prennent leurs responsabilités

Dernière Minute !

(quand il n'y en a plus, il y en a encore)

Nouvelle vulnérabilité WMF

- Une nouvelle vulnérabilité WMF a été découverte dans GDI
- Corruption de mémoire via les fonctions ExtCodeRegion et ExtEscape
  - DoS des applications utilisatrices prouvé
  - Exécution de code arbitraire fort possible d'après l'ISC et SecurityFocus ... mais pas selon Microsoft

Pour plus d'informations

- Alerte SecurityFocus : http://www.securityfocus.com/bid/16167/info
- ISC Diary : http://isc.sans.org/diary.php?storyid=1031
- Microsoft Security Response Center Blog : http://blogs.technet.com/msrc/archive/2006/01/09/417198.aspx

Références et

Remerciements

Références

- http://en.wikipedia.org/wiki/Windows_Metafile
- http://www.docisland.org/~saad/ISC_wmf_faq_fr.html
- http://handlers.sans.org/tliston/WMFTech.pdf
- http://secunia.com/advisories/18255/

Remerciements

- HAPSIS, mon employeur
  - http://www.hapsis.fr/
- Damian “Jr. Gong” Marley et Robert Plant
  - pour la musique ;-)
- Et vous tous
  - pour m’avoir écouté !