



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Network+Interop 2004 Paris

Session *Vulnérabilités et gestion des correctifs de sécurité*
4 novembre 2004

Vulnérabilités : de la découverte à l'exploitation

Jean-Baptiste Marchand

[<Jean-Baptiste.Marchand@hsc.fr>](mailto:Jean-Baptiste.Marchand@hsc.fr)

- x Vulnérabilités : introduction
- x Cycle de vie des vulnérabilités
 - x Qui trouve des vulnérabilités et comment ?
 - x Quel est le processus suivi lorsqu'une vulnérabilité est rapportée à un éditeur ?
 - x Comment aboutit-on à la publication d'un correctif par l'éditeur ?
 - x Dans quel cas une vulnérabilité est exploitée, notamment à large échelle ?
- x Tendances des vulnérabilités du moment
- x Solutions face aux vulnérabilités
- x Références

- x Vulnérabilité : erreur de conception (*bug*) dans un **produit** ayant un impact sur la sécurité du système d'information
- x Vulnérabilités systèmes
 - x Par opposition aux vulnérabilités applicatives (ex : injection SQL, cross-site scripting dans les applications web)
- x Grandes classes de vulnérabilités systèmes
 - x Vulnérabilités des serveurs : vulnérabilités dans des logiciels serveurs
 - x Exemple 1 : service RPC des systèmes Windows (systèmes d'exploitation)
 - x Exemple 2 : extension ISAPI dans IIS 5.0 (logiciel serveur)
 - x Exemple 3 : firmware d'un équipement réseau
 - x Vulnérabilités des postes clients
 - x Vulnérabilités dans les logiciels couramment utilisés sur le poste client
 - x Récemment : navigateurs web (Internet Explorer, Mozilla), lecteurs multimédia (QuickTime, Real Player, Winamp), outils classiques (Explorateur Windows, Winzip, Acrobat Reader), ...

Qui trouve des vulnérabilités ?

- x La plupart du temps, des chercheurs en vulnérabilités
 - x Indépendants
 - x Il s'agit d'un domaine de recherche au même titre que d'autres domaines
 - x Les vulnérabilités sont également devenues source de revenus financiers
 - x Exemple 1 : Vulnerability Contributor Program d'iDEFENSE (<http://www.idefense.com/poi/teams/vcp.jsp>)
 - x Exemple 2 : fondation Mozilla qui récompense la découverte de vulnérabilités dans la suite de logiciels open-source Mozilla
 - x Dont c'est le métier
 - x Grands éditeurs en sécurité (eEye, NGS, ISS, Core-ST, Symantec, ...) ont un département employant des chercheurs en vulnérabilités.
- x Plus rarement, par les éditeurs de logiciels
 - x Souvent, la vulnérabilité est corrigée de façon silencieuse et n'est typiquement pas référencée
 - x Contre-exemple : MS00-062, 'Local Security Policy Corruption' Vulnerability

Comment sont trouvées les vulnérabilités ?

- x Nombreuses méthodes pour rechercher des vulnérabilités
 - x Audit de code source (applications dont le code source est disponible) ou du code désassemblé
 - x Typiquement, à l'aide d'outils recherchant certaines classes de vulnérabilités
 - x Ex : outils recherchant les appels à certaines fonctions connues comme pouvant poser des problèmes de sécurité si elles sont mal utilisées
 - x Tests sur le produit
 - x Outils testant de façon automatique le comportement d'un logiciel donné face à un large ensemble de données variées
 - x Ex : fuzzing pour détecter des vulnérabilités systèmes
 - x Reverse-engineering
 - x Y compris des correctifs de sécurité...
 - x Autres...

Que se passe t-il lorsqu'une vulnérabilité est découverte ?

- x Processus idéal :
 - x Informer l'éditeur de la vulnérabilité
 - x Les éditeurs disposent typiquement d'une adresse électronique dédiée aux rapports de vulnérabilités (ex : `secure@editeur.com`), traitée par un service de suivi des incidents
 - x Dans le cas d'un logiciel opensource, l'équipe de développement est directement contactée
 - x L'assistance d'une tierce-partie (par exemple, un CERT (Computer Emergency Rescue Team)) peut éventuellement être sollicitée
 - x Assister l'éditeur, pour confirmer, expliquer, reproduire et corriger la vulnérabilité
 - x Activité **bénévole**
 - x Attendre que l'éditeur fournisse un correctif et publie un bulletin de sécurité
 - x Ceci prend du temps, notamment lorsqu'il faut s'assurer que le correctif n'a pas des effets de bord au sein d'un logiciel complexe
 - x Ex : Upcoming Advisories d'eEye
<http://www.eeye.com/html/research/upcoming/index.html>

Lorsqu'une vulnérabilité est corrigée par un éditeur

- x Publication d'un correctif et d'un bulletin de sécurité
 - x L'éditeur remercie la société ou l'individu à l'origine de la vulnérabilité
 - x Un **avis de sécurité** peut également être publié, indépendamment de l'éditeur
 - x A discrétion de l'équipe qui a découvert la vulnérabilité, des **informations techniques détaillées** peuvent être publiées dans l'avis
 - x L'avis peut être accompagné d'un programme permettant de produire la vulnérabilité ou d'informations suffisamment détaillées pour l'écrire
 - x Les éditeurs poussent de plus en plus à ce que les chercheurs en sécurité laisse un délai avant publication de détails sur la vulnérabilité
 - x Laisser le temps pour l'application des correctifs (de 30 jours jusqu'à 3 mois)
 - x Approche représentée par l'OIS (Organization for Internet Safety), menée par les éditeurs majeurs mais avec **peu d'adhésion de la communauté sécurité** (<http://www.oisafety.com/adopters.html>)
 - x Parfois, aucun détail publié
 - x D'autres sources d'informations sont cependant disponibles, en premier lieu le correctif de sécurité binaire fourni par l'éditeur

Ce qui peut aussi arriver lorsqu'une vulnérabilité est découverte...

- x Publication d'une vulnérabilité sans correctif disponible
 - x La vulnérabilité est publiée sans prévenir l'éditeur
 - x Cas des vulnérabilités Internet Explorer de l'été 2004
 - x L'éditeur doit alors travailler rapidement à un correctif
- x Vulnérabilité non publiée et, a fortiori, non corrigée
 - x Exploitée de façon silencieuse, probablement par une communauté restreinte, à l'origine de sa découverte, éventuellement découverte suite à la compromission de systèmes
 - x Dans le jargon de la sécurité, il s'agit d'un **0day**
 - x Exemple 1 : vulnérabilité MS03-007 (vulnérabilité dans ntdll.dll, exploitable typiquement sur IIS 5.0 via WebDAV), découverte suite à la compromission de serveurs web IIS de l'U.S. Army mi-mars 2003
 - x Exemple 2 : vulnérabilités Internet Explorer exploitées pour l'installation de logiciels malveillants (ex : 180 Solutions Trojan en Juin 2004)

Où sont publiées et référencées les vulnérabilités ?

- × Les vulnérabilités sont annoncées dans des listes électroniques
 - × Exemples de listes : Bugtraq, Full-Disclosure, Vulnwatch, ...
 - × Reprises par de nombreuses listes de veille en vulnérabilités : Secunia, Securiteam, ...
- × Elles sont ensuite référencées à de nombreux endroits
 - × Bases de vulnérabilités des acteurs du monde de la sécurité
 - × Securityfocus (Symantec) BID, ISS X-Force database, OVSDB (The Open Source Vulnerability Database)
 - × Référentiel unique entre ces bases : CVE (Common Vulnerabilities and Exposure)
 - × Identification des vulnérabilités du type CAN-200x-id (candidats) ou CVE-200x-id (entrées validées)

Ce qui arrive après la publication d'une vulnérabilité

- x Publication d'un exploit
 - x Programme permettant de tester la vulnérabilité, en tentant de l'exploiter
 - x Attention, s'assurer que l'exploit fait bien ce qu'il prétend faire et pas autre chose..
 - x Tous les exploits ne sont pas égaux !
 - x Suivant la nature de la vulnérabilité, l'exploit peut être spécifique à une version donnée du logiciel
 - x Typiquement à cause d'adresses mémoire qui peuvent varier suivant les versions logicielles utilisées
 - x Un exploit dit "universel" fonctionnera sur plusieurs versions du logiciel (ex : différents Service Pack et différentes langues d'un système Windows)
 - x L'exploit peut être fourni par le découvreur de la vulnérabilité
 - x Il peut aussi être écrit de façon indépendante, en se basant
 - x sur les détails fournis dans l'avis initial
 - x sur une recherche menée par d'autres chercheurs en vulnérabilités
 - x sur le correctif de sécurité binaire fourni par l'éditeur
 - x sur les modifications apportées dans le code source des projets OpenSource

- x Devenir d'un exploit
 - x Intégré dans des scanners de vulnérabilités pour détecter l'application du correctif correspondant
 - x Explique en partie pourquoi les grands éditeurs de scanners de vulnérabilités (eEye, ISS, NGS) ont un département de recherche en sécurité
 - x Façon fiable de tester la protection contre une vulnérabilité donnée
- x Utilisation dans un logiciel malveillant (virus, vers, ...)
 - x Nombreux exemples : Slammer (janvier 2003), Blaster (été 2003), Sasser (mai 2004)
 - x D'autres fois, l'exploit n'est pas publié et une vulnérabilité devient directement un vers
 - x Cas de CodeRed (été 2001) ou de Witty (mars 2004)

Tendances des vulnérabilités du moment

- x Délai entre la publication d'un correctif et l'apparition d'un vers exploitant la vulnérabilité tend à se réduire
 - x 26 jours pour Blaster (Juillet-Août 2003), 1 jour pour Witty (18, 19 Mars 2004)
- x Les virus récents utilisent des vulnérabilités systèmes récentes pour se propager et infecter un maximum de systèmes
 - x Ex : variantes récentes de W32/Sdbot
- x Vulnérabilités des navigateurs web sont utilisées par la criminalité organisée
 - x Ex : Attaques de type phishing visant à collecter des informations confidentielles
- x Plusieurs produits commerciaux ou opensource de type boîte à outils pour exploiter les vulnérabilités
 - x CORE Impact, CANVAS (Immunity), Metasploit (Metasploit.org)

- x Assurer une veille en vulnérabilités
 - x Se tenir informé des nouvelles vulnérabilités
 - x Bien comprendre la portée des vulnérabilités et les risques associés
- x Travailler à des solutions correctives pour les vulnérabilités
 - x Analyse de risque impérative
 - x L'application du correctif est l'une des solutions à envisager
 - x Pas forcément réalisable dans l'urgence
 - x D'autres solutions envisageables
 - x Désactivation de la fonctionnalité à l'origine de la vulnérabilité
 - x Quid des vulnérabilités du poste client ?
- x Concevoir des architectures et des systèmes permettant de limiter la portée d'une vulnérabilité nouvellement découverte

- x Bases de vulnérabilités
 - x CVE (Common Vulnerabilities and Exposure) : <http://cve.mitre.org/>
 - x ICAT Metabase : <http://icat.nist.gov/>
 - x Virus : base de virus des éditeurs d'anti-virus
 - x VGrep : <http://www.virusbtn.com/resources/vgrep/index.xml>
- x Gestion des correctifs
 - x PatchManagement : <http://www.patchmanagement.org/>
- x Tendances des vulnérabilités exploitées sur l'Internet
 - x SANS Top 20 Vulnerabilities : <http://www.sans.org/top20/>
 - x Symantec Internet Security Threat Report
 - x <http://enterprisesecurity.symantec.com/article.cfm?articleid=4776> (résumé)
 - x <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>