Protecting Against the 0-day Exploit

IT Security Office
University of Iowa
October 4, 2006

Agenda

- What is a 0-day Exploit
- 0-day Exploit targets
- Why are 0-day Exploits bad
- Latest 0-day Exploits
  - WebViewFolderIcon setslice
  - Mozilla Firefox Javascript Vulnerabilities – False Alarm
  - Internet Explorer VML Exploit
- Live Demo of the IE VML Exploit
- Best Practices for preventing 0-day Exploits
- Open Discussion

What is a 0-day Exploit

- A zero-day exploit is one that takes advantage of a security vulnerability on the same day or before the vulnerability becomes publicly released
- It's a new, unknown vulnerability which is difficult to guard against. --Brent Huston (ITWorld.com)
- 0-day exploits are mainly based on a Proof-of-Concept

Why are 0-day Exploits bad

- Difficult to detect
- Lack of understanding how the exploit works
- Protecting against the unknown is difficult
- Time between the release of the exploit and the vendor response is very critical

0-day Exploit Targets

- Instant Messenger Applications: AIM, Jabber, MSN, Google Talk, ICQ, etc.
- Web Browsers: Internet Explorer, Mozilla Firefox, Opera, etc.
- Others: Document Types (.doc, .ppt, .xls, .mdb …), pdf viewers, image viewers, multimedia players, p2p applications.
- Operating Systems and Services: Windows, Mac OS X, *nix, DNS, DHCP, etc.

Latest 0-day Exploits

- WebViewFolderIcon setslice
  - Microsoft WebViewFolderIcon ActiveX control is prone to a buffer-overflow vulnerability.
  - The underlying cause of the setSlice vulnerability is an integer overflow in COMCTL32.DLL, a core Windows component used by a large number of applications. -- Alex Sotirov (Determina)
    - 7/18/2006 – Initially released as a Denial of Service
    - 9/2006 – Code executing variant released by the author
    - 9/26/2006 – Exploit Code Published
    - 9/28/2006 – Microsoft Published Security Advisory (926043)
    - 9/29/2006 – Determina released a free patch
    - 10/10/2006 – Scheduled patch by Microsoft

Latest 0-day Exploits (Cont.)

- Mozilla Firefox Javascript Vulnerabilities
  - Mischa Spiegelmock and Andrew Wbeelsoi announce that they have discovered 30 different vulnerabilities in Firefox 1.5.0.7 at ToorCon 2006
  - Mozilla Firefox is prone to multiple unspecified JavaScript vulnerabilities because the application fails to properly sanitize user-supplied input before using it to create new JavaScript objects.
    - 10/1/2006 – Security Focus assigns BID 20294 and identifies the vulnerabilities as Mozilla Firefox Unspecified Javascript Remote Code Executuion
    - 10/3/2006 – The BID is retired because the researchers have claimed that their original reports were incorrect.

Latest 0-day Exploits (Cont.)

- Internet Explorer VML Exploit
  - The Vector Markup Language is XML-based language used to draw vector graphics – VML graphics
  - The vulnerability consists of unchecked buffer in VML rendering and uses stack-based overflow
  - Rated Critical for Windows 2000, Windows XP(SP1/SP2), Windows 2003 (Windows 2003SP1 – Moderate)
  - Impact of the attack – remotely exploitable and it can run code in the security content of the logged on user
  - Attack Vectors – Specially crafted HTML e-mail and malicious web sites

Latest 0-day Exploits (Cont.)

- Internet Explorer VML Exploit (Cont.)
  - 9/18/2006 – Vulnerability published by Adam Thomas (Sunbelt Software)
  - 9/19/2006 – Microsoft Published Security Advisory (925568)
  - 9/20/2006 – Active Exploit against VML in the wild
  - 9/22/2006 – Third party patches released and workarounds released by Microsoft
  - 9/27/2006 – Microsoft released and out of cycle patch to fix this vulnerability

Live Demo - Systems

- Victim Windows XP SP2
  - Fully Patched (well… mostly)
  - AV Up-to-date
- Attacker FreeBSD
  - IRC Server
  - Web Server
  - FTP Server

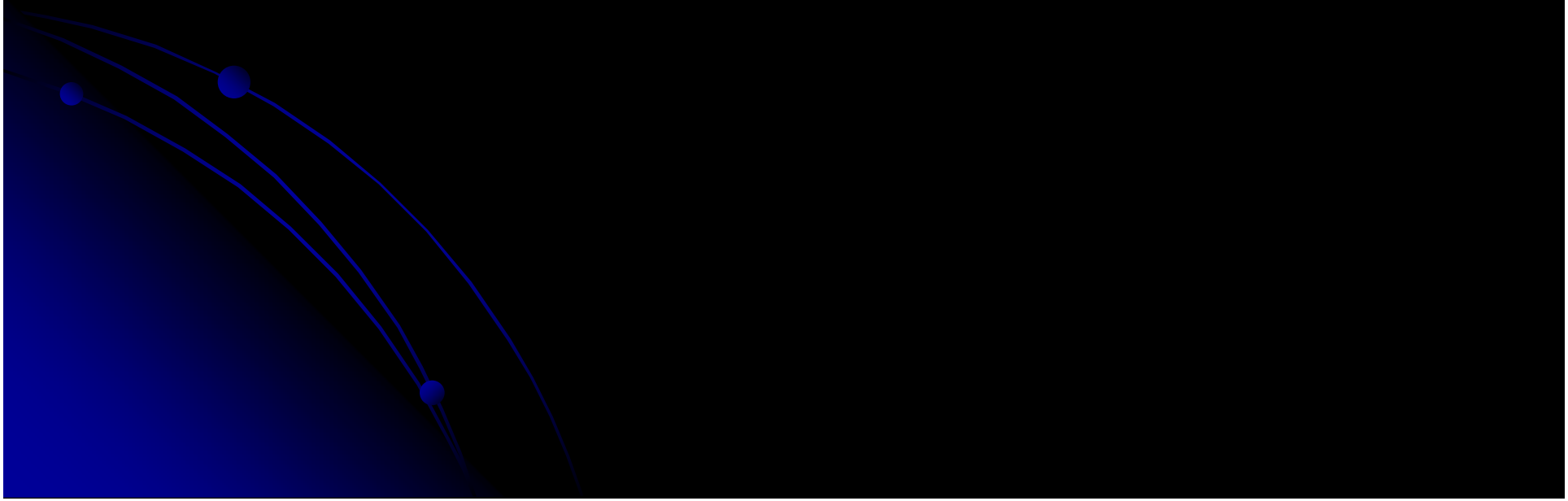
Live Demo – Attack Scenarios

Two User Scenarios

- User Privileges
- Administrator Privileges

- User visits malicious website.
- Website exploits VML vulnerability in victim's browser.
- Bot and attack script is download and run
- Impact Analysis

Live Demo



Prevent Zero Day Exploits

- Defense In Depth

- Run without Administrator Privileges
- Data Execution Prevention DEP
- Anti-Virus
- Host Firewall
- Targeted Mitigation

“It’s better to use non-admin WITHOUT AV than use admin WITH anti-virus.”

Why?

“Almost all malware will not work if run with non-admin privileges”

Aaron Margosis’ Weblog

Why Reduce Privileges?

- As Administrator Malware Can
  - Hide from anti-virus
  - Disable or Delete anti-virus
- Protection from ourselves – Human Error
  - Virus & Phishing attacks require interaction
  - Don’t invite malware to use Administrator privileges

Don’t Give Malware Admin

- Install kernel-mode rootkits or keyloggers (impossible to detect)
- Install and start services
- Install ActiveX controls (Spyware / Adware)
- Use privileges to access other computers over a network
- Access data belonging to others
- Execute code at logon (Trojan Horse)
- Access LSA Secrets, possibly including info for domain accounts
- Erase logs including security logs
- Destroy data and OS

How to Reduce Privileges

- Run as standard user
  - Not Administrator or Power User
  - Use Runas or sudo for privileged commands
- Run Internet applications as standard user
  - Web browsers, e-mail, IM
  - Any software that handles un-trusted data
  - Use Runas or DropMyRights

Data Execution Prevention

- DEP buffer overflow protection
  - In Memory DEP marks data as not executable
- Hardware DEP – enabled in BIOS and OS
  - AMD No eXecute - NX
  - INTEL eXecute Disable - XD
- Software DEP – Emulation Mode
  - XPSP2, W2K3SP1, Linux 2.6.7
  - Defaults to “essential programs and services”
  - Enable for all programs
  - Doesn’t this imply IE is not essential?

Anti-Virus

- Keep AV Current and Definitions updated
- Can AV detect Zero Day exploits?
  - Exploit may act like a known virus
  - AV may detect general suspicious activity
- Review AV Logs
- Don’t Depend Only on Anti-Virus
- Check out Heuristic AV like NOD32

Host Firewall

- Reduce Exploit Appeal & Network Exposure
- Firewalls protect from worms
  - Not when joined to a domain
- Scope your firewall rules
  - Allow specific hosts or networks
- Outbound firewalls
  - Prevent Malware from connecting to C&C
  - Alerts you of suspicious activity

Mitigation

- Trusted Patches – ECM SMS
- Third Party Patches
- Un-register DLL
- ActiveX KillBit
- Zero Day workarounds
  - May break features
  - May prevent patches from installing

Discussion

- Strategies to Prevent Zero Day Attacks
- Information and Resources
- What works? What doesn’t work?