



Vulnerability Summary

January 2004

Paul Asadoorian
IT Security Specialist
Brown University

Vulnerabilities

- Linux Kernel Vulnerabilities
- Phishing with Internet Explorer
- MDAC Buffer Overflow
- Printer Soap Box
- Trends and Fun Stuff

Linux Kernel Vulnerabilities

- Two vulnerabilities:
 - do_brk() function contains integer overflow
 - mremap privilege escalation
- Both provide for local root access
- 2.2, 2.4 and 2.6 series are vulnerable
- Actively being exploited

Linux Kernel Vulnerabilities

Defense

- Refer to your vendor for patches
- Latest stable kernel versions:
 - 2.6.1
 - 2.4.24
 - 2.2.25

Linux Kernel Vulnerabilities

- do_brk()
 - <http://security.nnov.ru/search/news.asp?binid=3289>
- mremap
 - <http://security.nnov.ru/search/news.asp?binid=3344>
- <http://www.kernel.org> – Latest kernel downloads

Phishing with Internet Explorer

- URL redirection
- Used quite often to harvest credit card numbers
- Great fun, just watch!



Phishing with Internet Explorer

Defense



- No Patch
- Careful where you click
- Use another browser

Phishing with Internet Explorer

- Mozilla Project

- <http://www.mozilla.org/> (New Version 1.6 - January 15, 2004)

- Opera

- <http://www.opera.com/> (New Version 7.23, January 2004)

- Guides to securing IE:

- <http://www.computerstuff.net/security/ieconfig.htm>
- <http://www.sans.org/rr/paper.php?id=287>



Phishing with Internet Explorer

- Links:

- <http://www.kb.cert.org/vuls/id/652278>
- <http://security.nnov.ru/search/news.asp?binid=3110>
- <http://www.theregister.co.uk/content/55/34447.html>



MDAC Buffer Overflow

- Buffer Overrun in MDAC Function Could Allow Code Execution
- Attacker must respond to a broadcast request
- MDAC (Microsoft Data Access Components) are used for database communications

MDAC Buffer Overflow

- Following are vulnerable:
 - Microsoft Windows 2000
 - Windows XP
 - SQL Server 2000
 - Windows Server 2003 (incl. 64-bit edition)
 - Microsoft Data Access Components 2.5, 2.6, 2.7, 2.8
 - Installs with Microsoft Windows NT 4.0 Option Pack, Microsoft Access, and SQL Server

MDAC Buffer Overflow

Defense

- Apply patches
- Block UDP port 1434 on network and client
 - Prevent client from broadcasting

MDAC Buffer Overflow

- Links:
 - <http://www.microsoft.com/technet/security/bulletin/MS04-003.asp>
 - <http://www.kb.cert.org/vuls/id/139150>
 - <http://security.nnov.ru/search/news.asp?binid=3066>

Printer Soap Box



Printer Soap Box

- Weak security leads to:
 - Attackers storing files on printers
 - Changing any and all configuration
 - Changing the display
 - Locking the display
 - Using printers as portscanners
 - Gathering network information
 - Using printers as a proxy server

Printer Soap Box



- Phenoelit group
- Easy to use GUI

Printer Soap Box

Defense

- Update firmware
- Filter from Internet/Campus
- Turn off unnecessary services:
 - Telnet
 - SNMP
 - FTP

My Take On MyDoom

- Best write-up
 - <http://www.f-secure.com/v-descs/novarg.shtml>
- Propagation (Fastest spreading)
 - Email
 - P2P Networks
- Signs of infection:
 - Notepad open with garbage characters
 - Various registry entries

My Take On MyDoom

- Payload:
 - SPAM Relay (It's own SMTP server, easier to block than using another relay)
 - DDoS www.sco.com (By DNS Name, Expires on Feb. 12th)
 - New variant (MyDoom.B) attacks www.microsoft.com too
 - **Backdoor (TCP Proxy and Upload more malicious code)**

Paul's Pick Of The Month

“A visit from the FBI”

<http://www.theregister.co.uk/content/55/35175.html>

“A favorite trick is to surreptitiously turn on the Webcam of an owned computer in order to watch the dupe at work, or watch what he's typing on screen.”

“Hey, put your shirt back on!”

Paul's 2004 Predictions



- SPAM will increase, as will propagation methods
- SSL VPN's will become more popular, hackers will take notice
- SCO will sue more people (until it runs out of money)

/* The End */



- Other cool links:

- <http://packetstormsecurity.nl/>

- <http://www.security.nnov.ru/>

- <http://www.cert.org>

- <http://www.whitehats.com>

- <http://rr.sans.org>

- <http://www.incidents.org>

- <http://www.astalavista.com/>

