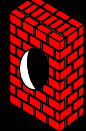
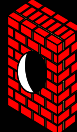
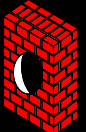
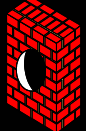
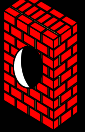
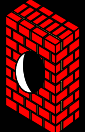

Vulnerability Summary

August 2004



Paul Asadoorian
Lead IT Security Specialist
Brown University

Vulnerabilities

- Adobe Acrobat ActiveX Control Buffer Overflow 
- Unpatched Internet Explorer Vulnerabilities Update 
- Netgear Remote Root Shell 
- AOL Instant Messenger Buffer Overflow 
- Multiple Vulnerabilities in libpng 
- SSH Remote Root Password Brute Forcing 

Adobe Acrobat ActiveX Control Buffer Overflow

- Attacks Acrobat via the web browser
- A specially crafted URL will cause a buffer overflow:
 - `GET /any_existing_dir/any_existing_pdf.pdf%00[long string] HTTP/1.1`
- Clicking on the link causes the overflow

Adobe Acrobat ActiveX Control Buffer Overflow

- Adobe appears to have silently fixed the bug
- Exploit code will still crash the application
- It seems to do that well on its own anyhow
- UNIX Variants have vulnerabilities too

Adobe Acrobat ActiveX Control Buffer Overflow

- Why is this so bad?
 - It is browser independent
 - Almost every PC has this installed
 - Vendor did not announce it as a problem

Adobe Acrobat ActiveX Control Buffer Overflow

- Upgrade to the latest version of Adobe Acrobat
- Tell Acrobat not to open in browser:
 1. Open Adobe Acrobat/Acrobat Reader
 2. Go to Edit --> Preferences
 3. Uncheck the "Display PDF in browser" setting
 4. Click OK

NOTE: If you do this acrobat will not automatically open PDFs from a web page.

Adobe Acrobat ActiveX Control Buffer Overflow

- Original Advisory:
 - <http://www.security.nnov.ru/search/news.asp?binid=3912>
- iDEFENSE Advisory for Windows:
 - <http://www.odefense.com/application/poi/display?id=126&type=vulnerabilities>
- iDEFENSE Advisory for UNIX:
 - <http://www.odefense.com/application/poi/display?id=124&type=vulnerabilities>
- Adobe Acrobat Homepage:
 - <http://www.adobe.com/products/acrobat/>

Unpatched Internet Explorer

Vulnerabilities Update

- Use of “Styles” and drag and drop functionality to install malware
- Allows access to the windows startup folder
- Variation ties it to the scrollbar for easy installation without user knowledge

Unpatched Internet Explorer

Vulnerabilities Update

- Both Windows XP SP1 & SP2 vulnerable
- Not recognized as a vulnerability by Microsoft
- No patches available
- SP2 potential workaround is to disable “binary behaviors”

Unpatched Internet Explorer

Vulnerabilities Update

- For general web browsing, use an alternative browser:
 - Mozilla (<http://www.mozilla.org>)
 - *Firefox (<http://www.mozilla.org/firefox>)
 - Opera (<http://www.opera.com>)

** Firefox is my personal favorite, fast, tabbed browsing, etc...*

Unpatched Internet Explorer



Vulnerabilities Update



“IE: Internet Exposure - Internet Explorer Vulnerabilities and What You Can do About Them”

<http://www.pauldotcom.com/InternetExposure.pdf>

Unpatched Internet Explorer



Vulnerabilities Update



- Download.Ject-style worm spreads via IM

- <http://www.securityfocus.com/news/9372>

- Security Holes Sinking IE

- <http://www.eweek.com/article2/0,1759,1624514,00.asp>

“Unrestricted client-side active scripting is the future of virus delivery, industrial espionage and cyber-terrorism.”

Unpatched Internet Explorer



Vulnerabilities Update



- New, Fixed, and Unrelated IE bugs:
 - <http://www.us-cert.gov/cas/techalerts/TA04-212A.html> -
- Original posting by http-equiv:
 - <http://archives.neohapsis.com/archives/ntbugtraq/2004-q3/0125.html>
- Proof of Concept Exploits
 - Warning: Clicking these links will launch the PoC Exploits
 - <http://www.malware.com/wottapoop.html>
 - <http://www.mikx.de/scrollbar/> - Uses scrollbar activity to drop file

Unpatched Internet Explorer



Vulnerabilities Update



- Various other postings:
 - <http://archives.neohapsis.com/archives/fulldisclosure/2004-08/0822.html>
 - <http://archives.neohapsis.com/archives/fulldisclosure/2004-08/0842.html>
 - <http://archives.neohapsis.com/archives/fulldisclosure/2004-08/0938.html>
 - <http://archives.neohapsis.com/archives/fulldisclosure/2004-08/0942.html>
- SecurityFocus BID
 - <http://www.securityfocus.com/bid/10973>
- Secunia Advisory:
 - <http://secunia.com/advisories/12321>

Netgear Remote Root Shell

- Two new remote vulnerabilities
- Netgear model DG834G Wireless router/firewalls are vulnerable
- Allows unauthorized remote root access



Netgear Remote Root Shell

- To exploit:
 - Telnet to 192.168.0.1 2602
 - Password “zebra”
 - Go to <http://192.168.0.1/setup.cgi?todo=debug>
 - Then telnet to port 23
- Securityfocus claims accessibility via WAN port

Netgear Remote Root Shell

- Finding bugs in home firewalls:

```
# strings dg834_a1_03_00.img | grep zebra  
zebra
```

- Sometimes contents is encrypted
- Sometimes you're surprised what you find

Netgear Remote Root Shell

- Original Advisory:
 - <http://www.security.nnov.ru/search/news.asp?binid=3915>
- Securityfocus vulnerability:
 - <http://www.securityfocus.com/bid/10935>
- Product Information:
 - http://www.netgear.com/products/prod_details.php?prodID=223&view

AOL Instant Messenger Buffer Overflow

- All versions of AIM appear to be vulnerable
- Buffer overflow in the “Away” function
- Exploitable via a specially crafted URL (e.g. “aim:<url>”)

AOL Instant Messenger Buffer Overflow

- Fun with Vulnerability disclosure:
 - iDEFENSE finds bug in July and works solely with vendor
 - Workaround is found, but still kept secret
 - Secunia finds bug, announces to world before AOL or iDEFENSE
 - Oops!

AOL Instant Messenger Buffer Overflow

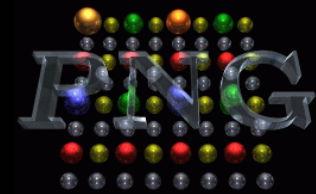
- Remove the following registry key:
 - HKEY_CLASSES_ROOT\aim
- iDEFENSE script:
 - Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKCR\aim\"

AOL Instant Messenger Buffer Overflow

- Cert Advisory:
 - <http://www.kb.cert.org/vuls/id/735966>
- Secunia Advisory:
 - <http://secunia.com/advisories/12198/>
- iDEFENSE Advisory:
 - <http://www.idefense.com/application/poi/display?id=121&type=vulnerabilities>

Multiple Vulnerabilities in libpng

- PNG – Portable Network Graphics format
- Meant to replace GIF and to some extent TIFF image formats
- Completely Open Source, whereas other formats may not be



Multiple Vulnerabilities in libpng

- Numerous operating systems and devices are vulnerable
- Must introduce a malformed image to the application
- Get user to go to a web page

Multiple Vulnerabilities in libpng

- Most Linux variants and Mac OS X are vulnerable
- Patches are available from most vendors
- libpng version [1.2.6rc1](#) is the latest version and contains all fixes

Multiple Vulnerabilities in libpng

- US-CERT Technical Cyber Security Alert:
 - <http://www.us-cert.gov/cas/techalerts/TA04-217A.html>
- PNG Homepage:
 - <http://www.libpng.org/pub/png/>
- Original Vulnerability Findings:
 - <http://scary.beasts.org/security/CESA-2004-001.txt>

SSH Remote Root Password Brute Forcing

- Increased SSH scanning activity
- Host logs showed repeated login attempts
- Security community was on the lookout for a new SSH scanning tool

SSH Remote Root Password Brute Forcing

- Brutessh2 was released and posted
- Tests for more than 2000 different passwords on root account
- Mystery solved...

SSH Remote Root Password Brute Forcing

```
/*
*the first brutessh was only for users guest & test
*brutessh2 is a brute for sshd port wich atempts to
login as root trying more than 2000 passwords for
it.
*users guest , test , nobody and admin with no
passwords are included.
*feel free to add more passwords and more users:=)
* <snip>
*For mass use a synscan :
*Eg: ./biggssh sship.txt
*Ok.Try This : Hostname root:12345
*/
```

SSH Remote Root Password Brute Forcing

- Do not allow root logins remotely:
 - “PermitRootLogin no” in sshd_config
- Watch your Auth logs closely

```
Aug 24 05:53:39 monkey sshd[1310]: Failed  
password for root from MY.SUB.NET.97 port  
1486 ssh2
```

- Use good passwords, change them often

SSH Remote Root Password Brute Forcing

- New Exploit Code:
 - <http://www.k-otik.com/exploits/08202004.brutessh2.c.php>
- Incident Storm Center Reports:
 - <http://www.incidents.org/diary.php?date=2004-08-2&isc=19c22d993a5d5f7d0efa8d1e438bdc8e>
 - <http://www.incidents.org/diary.php?date=2004-08-4&isc=526ce686f7a0df94abdee4f2cc3c0d40>

Article Of The Month

“New worm spies on you”

http://zdnet.com.com/2100-1105_2-320592.html

“Whether this worm is the work of professional snoopers or lusty teenagers--it's hard to say for certain.”



/* The End */

Questions? Comments? Flame Mail?

Paul_Asadoorian@brown.edu

This presentation:

<http://www.brown.edu/Research/SysAdmins/vuln-aug-2004.pdf>

Paul's Essential Security Links

<http://packetstormsecurity.nl/>

<http://www.incidents.org>

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

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

<http://www.cert.org>

<http://www.l0t3k.org/>

<http://www.whitehats.com>

<http://www.securiteam.com/>

<http://rr.sans.org>