
Vulnerability Summary

October 2003



Paul Asadoorian
IT Security Specialist
Brown University

Vulnerabilities

- Internet Explorer Fixes (Hurray!)
- 5 New MS Security Alerts (MS03-041-045)
- AOL Instant Messenger buffer overflow
- Multiple Bugs in OpenSSL
- New Trends and fun stuff

Internet Explorer

MS03-040

- IE versions 5.0.1, 5.5, and 6.0
- Cumulative patch, with 2 new fixes:
 - Object-Type identification in pop-up
 - Object-Type identification in XML
- Both all for remote code execution

Internet Explorer Fixes

- Defense:
 - Patch your browser (Windows Update)
 - EVEN IF YOU USE ANOTHER BROWSER
 - Don't allow users to login as administrator
 - Use another Browser:
 - Opera
 - Mozilla
 - Tweak Browser settings to disallow misbehaving web pages (ActiveX)
 - Run Host-Based IDS
 - OSIRIS (<http://osiris.shmoo.com/>) ← **FREE**
 - Be suspicious of all web sites

Internet Explorer

MS03-040

- Mozilla Project

- <http://www.mozilla.org/> (New Version 1.5 - October 15, 2003)

- Opera

- <http://www.opera.com/> (New Version 7.21, October 14, 2003)

- Guides to securing IE:

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

- Unpatched IE Vulnerabilities

- <http://www.pivx.com/larholm/unpatched/> (No longer in service)

Internet Explorer

MS03-040

- What, no unpublished vulnerabilities?
 - “Recently, we have seen a sea change in Microsoft’s commitment to rid its IE browser of the vulns that PivX Solutions and other third party researchers have identified. Given Microsoft’s recent positive actions together with the current rise in attacks against IE we have agreed to give Microsoft a good faith reprieve and have taken down our ‘Unpatched’ page.”
- Awwwwwww.....

MS Security Alerts (MS03-041-045)

- MS03-041 - Authenticode Verification
- MS03-042 – Troubleshooter Remote Buffer Overflow
- MS03-043 – Remote Buffer Overflow in Messenger
- MS03-044 – Remote Buffer Overflow in Windows Help
- MS03-045 – Buffer Overflow in Listbox

MS03-041 - Authenticode Verification

- NT, 2000, XP, 2003 using Outlook or Internet Explorer
- ActiveX control accesses the Authenticode vulnerability
- Allows for remote code execution

MS03-042 – Troubleshooter

Remote Buffer Overflow

- Only affects Windows 2000 Service Pack 2, 3, or 4 using Outlook or Internet Explorer
- Buffer overflow in ActiveX control (Tshoot.ocx)
- Allows remote code execution

MS03-041 & MS03-042

Defense

- Defense:
 - Apply Patches
 - EVEN IF YOU USE ANOTHER BROWSER/Email Client
 - Don't allow users to login as administrator
 - Use another Browser:
 - Opera
 - Mozilla
 - Tweak Browser settings to disallow misbehaving web pages (ActiveX)
 - Run Host-Based IDS (They catch this stuff)
 - OSIRIS (<http://osiris.shmoo.com/>) ← **FREE**
 - Be suspicious of all web sites

MS03-043 – Remote Buffer Overflow in Messenger

- Windows NT, 2000, XP, 2003 messenger services
- **Scarier than the new Texas Chainsaw Massacre:**
 - “Messenger Service does not properly validate the length of a message before passing it to the allocated buffer. “

MS03-043 – Remote Buffer Overflow in Messenger

- Defense:
 - Apply Patches
 - Block NetBIOS ports (135-139, 445)
 - Turn off messenger service
 - Most have done this to prevent POP-UP SPAM
 - Windows 2003 – Messenger turned off by default (Hurray!)

MS03-044 – Remote Buffer Overflow in Windows Help

- Windows NT, 2000, XP, 2003 IE or Outlook based attack
- HCP protocol contains buffer overflow
- Requires user visit web page to trigger

MS03-044 – Remote Buffer Overflow in Windows Help

- Defense:
 - Apply patches
 - Don't allow users to login as administrator
 - Deregister the HCP Protocol
 - Be suspicious of all web sites

MS03-045 – Buffer Overflow in Listbox

- Windows NT, 2000, XP, 2003
- Local exploit that uses User32.dll buffer overflow
- Must be interactively logged in

MS03-045 – Buffer Overflow in Listbox

- Defense
 - Apply patches
 - Run Host-Based IDS
 - OSIRIS (<http://osiris.shmoo.com/>) ← **FREE**

MS Security Alerts (MS03-041-045)

- Links

http://www.microsoft.com/security/security_bulletins/20031015_windows.asp

Microsoft Security Bulletin MS03-041 -

<http://www.microsoft.com/technet/security/bulletin/MS03-041.asp>

Microsoft Security Bulletin MS03-042 -

<http://www.microsoft.com/technet/security/bulletin/MS03-042.asp>

Microsoft Security Bulletin MS03-043 -

<http://www.microsoft.com/technet/security/bulletin/MS03-043.asp>

Microsoft Security Bulletin MS03-044 -

<http://www.microsoft.com/technet/security/bulletin/MS03-044.asp>

Microsoft Security Bulletin MS03-045 -

<http://www.microsoft.com/technet/security/bulletin/MS03-045.asp>

<http://www.cert.org/advisories/CA-2003-27.html>

AOL Instant Messenger buffer overflow

- AIM 5.2.3292 for Windows (Maybe others)
- Via a browser you can invoke the AIM protocol and access buffer overflow
 - See the trend...
- Buffer overflow exists in the username field
- Allows for remote code execution

AOL Instant Messenger buffer overflow

- Defense:
 - Upgrade AOL AIM, although I could not find a newer version or patch
 - Use alternative messaging software (Like Trillian <http://www.ceruleanstudios.com/>)
 - Run Host-Based IDS
 - OSIRIS (<http://osiris.shmoo.com/>) ← **FREE**

AOL Instant Messenger buffer overflow

- Links:
 - <http://www.security.nnov.ru/search/document.asp?docid=5254>
 - <http://www.aim.com> – Could not find the patch they are referring to.

Multiple Bugs in OpenSSL

- OpenSSL prior to 0.9.7c or 0.9.6k are vulnerable
- Buffer Overflow in the handling of ASN.1 encoded messages
- Many things use ASN.1 encoding (SNMP, X.509 certificates)

Multiple Bugs in OpenSSL

- Defense:
 - Upgrade to OpenSSL 0.9.7c or 0.9.6k
 - Upgrade software from your vendor
 - Don't use SSL for application that require above average security

Multiple Bugs in OpenSSL

- Links:

http://www.openssl.org/news/secadv_20030930.txt

<http://www.kb.cert.org/vuls/id/255484>

<http://www.kb.cert.org/vuls/id/104280>

<http://www.cert.org/advisories/CA-2003-26.html>

<http://www.uniras.gov.uk/vuls/> - Good write-up
by the group that found the vulnerabilities

Notice a Trend?

- Browser-Based exploits are popular
 - Buried in gigabytes of outgoing HTTP traffic
- Not blocked by firewall, missed by IDS
- Anti-Virus is no help
- P2P and messaging applications

New Strategy

- Patch quickly and more efficiently
- Use Host-Based IDS
- Investigate Intrusion Prevention technologies
- As a user, be more aware

Hack-Of-The-Month

Vampire Hackers Attack!

Romania Emerges As Nexus of Cybercrime

“...Pay me off or I'll sell the station's data to another country and tell the world how vulnerable you are. Proving it was no hoax, the message included scientific data showing the extortionist had roamed freely around the server, which controlled the 50 researchers' life-support systems.”

<http://www.theledger.com/apps/pbcs.dll/article?AID=/20031020/API/310201043>

/* 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>

