
Vulnerability Summary

February 2004

Paul Asadoorian
IT Security Specialist
Brown University



Vulnerabilities

- ZoneAlarm buffer overflow
- WINS buffer overflow
- Multiple Internet Explorer bugs
- Microsoft Virtual PC for Mac improper file validation
- Microsoft ASN.1 Library

ZoneAlarm buffer overflow

- Systems Affected:
 - ZoneAlarm 4.0 to 4.5.538.000
 - ZoneAlarm Pro 4.0 to 4.5.538.000
 - ZoneAlarm Plus 4.0 to 4.5.538.000
 - Zone Labs Integrity Client 4.0 to 4.5.084
- Comes with an email virus checker
- Overflow in “RCTP TO” field in SMTP engine
- “RCTP TO” is the recipient field of an email

ZoneAlarm buffer overflow

- Defense:
 - According to Zone Labs Security Advisory:

ZoneAlarm, ZoneAlarm Plus, and ZoneAlarm Pro users should upgrade to version: 4.5.538.001.

To update your Zone Labs client product:

1. Select Overview > Preferences.
2. In the Check for Updates area, choose an update option.

ZoneAlarm buffer overflow

- Links:
 - <http://www.eeye.com/html/Research/Advisories/AD20040219.html>
 - <http://www.eeye.com/html/Research/Upcoming/20040213-2.html>
 - <http://download.zonelabs.com/bin/free/securityAlert/8.html>
 - <http://secunia.com/advisories/10921/>

WINS buffer overflow

- WINS maps IP addresses to NetBIOS computer names
- Windows 2003 – causes DoS
- Windows NT & 2000 – ignores packets, but still vulnerable

WINS buffer overflow

- Defense
 - Apply patch (830352) Microsoft Security Bulletin MS04-006
 - Block ports 42/TCP and 137/UDP (WINS won't work though 😊)
 - Disable the WINS service

WINS buffer overflow

- Links:
- <http://www.microsoft.com/technet/security/bulletin/MS04-006.asp>
- <http://www.kb.cert.org/vuls/id/445214>

Multiple Internet Explorer bugs

- Three “new” vulnerabilities fixed
 - Travel Log Cross Domain Vulnerability
 - Function Pointer Drag and Drop Vulnerability
 - Improper URL Canonicalization Vulnerability
- This includes Phishing
- Replaces MS03-048 Security Bulletin

Multiple Internet Explorer bugs

- Vulnerabilities still remain:
 - http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/
 - 24 unpatched according to the above we site
 - Most deal with active scripting, ActiveX, etc..

Multiple Internet Explorer bugs

- 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>

Multiple Internet Explorer Bugs

- Defense
 - Patch
 - Use another Browser
 - Blah, blah.....

Ed Skoudis: Top 10 ways to fight Malware

1. Get an antivirus tool and keep it updated!
2. Get a personal firewall and/or Host-IDS.
3. Keep your systems patched.
4. Keep your browser security settings at Medium or even High.
5. Never click 'Yes' when asked if you want to install/run content from an organization you don't trust.

Ed Skoudis: Top 10 ways to fight Malware

6. Install an anti-spyware tool
7. Don't install a search-help bar in your browser unless it's from someone you trust.
8. Check to see which software certificates you're configured to trust.
9. Get a credit card to use solely for Internet purchases.
10. Don't run executable email attachments, even if sent by a friend.

<http://www.techtv.com/screensavers/answerstips/story/0,24330,3609685,00.html>

Microsoft Virtual PC for Mac improper file validation

- Affected products:
 - Microsoft Virtual PC for Mac 6.01, 6.1, 6.0, 6.02
- VM allows windows to run on OS X
- Allows local root privileges through local setuid file creation
- Allows non-root user to create and delete files with root permissions

Microsoft Virtual PC for Mac improper file validation

- Defense:
 - Patch
 - <http://www.microsoft.com/technet/security/bulletin/MS04-005.asp>
 - Original advisory
 - <http://www.atstake.com/research/advisories/2004/a021004-1.txt>

Microsoft ASN.1 Library

- 2 flaws in the ASN.1 library (MSASN1.DLL)
- ASN.1 is used in binary representation
- Remote exploit, DoS exploit already exists
- Windows NT 4.0, 2000, 2003, and XP affected

Microsoft ASN.1 Library

- Defense
 - Patch, Patch, and Patch
 - Many different methods of accessing this library

Other Vulnerabilities

- SNMP information leak in Linksys
 - Not confirmed by the vendor
- Multiple bugs in Oracle
 - Wait, I thought it was impenetrable Larry?
- Checkpoint VPN-1/SecureClient buffer overflow

Other Vulnerabilities

- Checkpoint Firewall-1 format string bugs
- Ipswitch IMail buffer overflow
 - Increased scanning for port 389
- Mac OS X Safari fails to properly display URLs in the status bar
- Mac OS X contains vulnerability in DiskArbitration when initializing writable removable media

Headlines Of The Month

“Microsoft cracks down on spread of source code”

<http://www.msnbc.msn.com/id/4305329/>

“Software giant sending out warning letters”

Headlines Of The Month

“FBI warning labels to appear on CDs,
DVDs, software”

<http://www.cnn.com/2004/TECH/ptech/02/20/downloading.music.ap/index.html>

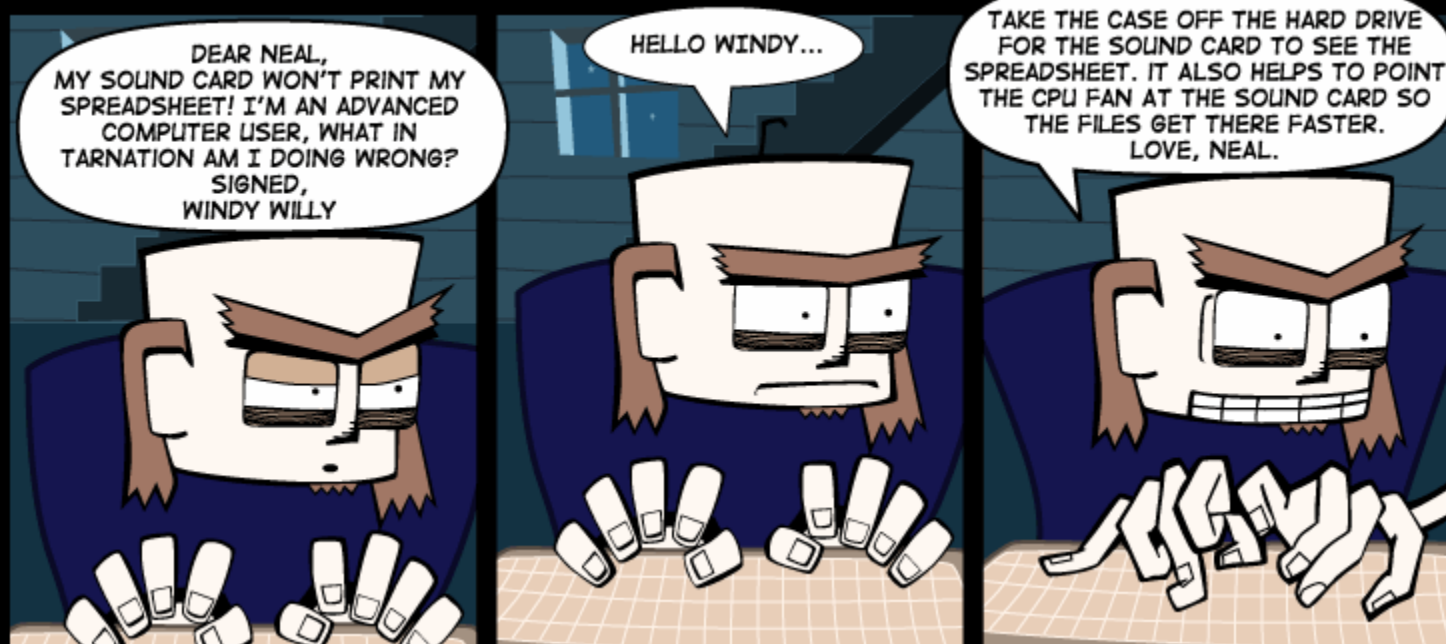
Headlines Of The Month

Mom sues RIAA members for racketeering

<http://www.theregister.co.uk/content/6/35663.html>

Funny Web Site Of The Month

NEAL'S HELPFUL HINTS!!



<http://www.ubergeek.tv/>

/* 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/>

