
Vulnerability Summary

October 2004



Paul Asadoorian
Lead IT Security Specialist
Brown University



Vulnerabilities

- Microsoft Vulnerability Mayhem
- Buffer Overflow Explosion
- DoS, remote code execution, input validation
- Oh My!



Microsoft

Vulnerability in Microsoft ASP.NET

- Web-based attacks:
 - Bypass forms based authentication
 - Bypass Windows authorization
 - Unauthorized viewing secured content
- Workarounds available
- Details here:
 - <http://www.microsoft.com/security/incident/aspnet.aspx>
- Original Advisory
 - <http://www.security.nnov.ru/search/document.asp?docid=6870>

Microsoft Security Bulletin

MS04-028

- Issued on Sept 12th, updated Oct 12th
- Buffer Overrun in JPEG Processing (GDI+)
- Affected software includes most Microsoft products
- User needs to access a JPG file
- GDIScan tool from SANS looks for all vulnerable libraries <http://isc.sans.org/gdiscan.php>

Microsoft Security Bulletin

MS04-029

- Vulnerability in RPC Runtime Library
- Allows for information disclosure and DoS
 - Read portions of memory
- Replaces several previous patches
- Windows NT Only

Microsoft Security Bulletin

MS04-030

- Vulnerability in WebDAV XML Message Handler
- DoS only, but takes down web server
 - Who cares, right?
- Affected software – Windows 2000/2003 and XP

Microsoft Security Bulletin

MS04-031

- Vulnerability in NetDDE Could Allow Remote Code Execution
 - Low worm potential according to SANS
- NT/2000/2003/XP/98 Vulnerable
 - XP SP2 not vulnerable
 - Hmmmm, interesting.....
- NetDDE services are not started by default

Microsoft Security Bulletin

MS04-032

- Four Vulnerabilities in one:
 - Window Management Vulnerability
 - Virtual DOS Machine Vulnerability
 - Graphics Rendering Engine Vulnerability
 - Windows Kernel Vulnerability
- Graphics rendering in WMFs and EMFs similar to JPG vulnerabilities
- NT/2000/2003/XP/98 vulnerable
 - XP SP2 not vulnerable

Microsoft Security Bulletin

MS04-033

- Vulnerability in Microsoft Excel Could Allow Remote Code Execution
- Microsoft Office 2000 SP3, XP SP2
 - Excel 2000 & 2002 for Windows Vulnerable
 - Excel 2001 & v. X for Mac Vulnerable
- Allows for remote code execution, must force user to open excel file

Microsoft Security Bulletin

MS04-034

- Vulnerability in Compressed (zipped) Folders
- Could Allow Remote Code Execution
 - Must force user to open zip file
- XP/2003 Vulnerable

Microsoft Security Bulletin

MS04-035 & MS04-036

- Buffer Overflows in SMTP and NNTP
- Force SMTP server to receive malformed DNS response
 - Can be done with sending any packets to target
 - Block TCP port 53 (use caution!)
- NNTP remote code exploit

Microsoft Security Bulletin

MS04-037

- Vulnerability in Windows Shell
- Could Allow Remote Code Execution
- Must force user to visit web site
- NT/2000/2003/XP/98 Vulnerable
 - XP SP2 not vulnerable

Microsoft Security Bulletin

MS04-038

- Cumulative Security Update for Internet Explorer
 - Five remote code executions
 - Three information disclosures
- Covers all platforms, include XP SP2
- Tries to Fix some popular ones, like “Drag & Drop”, but doesn’t (!)

Blackhats at work



- September 23rd – October 7th
 - Multiple exploits released for GDI JPG buffer overflow
- October 15th
 - Proof-of-concept exploit for the Windows NNTP vulnerability (MS04-036)

Blackhats at work

- October 20th
 - A proof-of-concept (POC) exploit for MS04-030 has been made available.
 - IE unpatched bugs released:
 - Modified "drag & drop" exploit bypasses recent fix
 - All new bypass of the security zone restrictions



Defense



- Apply Patches
 - Enable Automatic Updates
 - Run Windows Update periodically
 - Verify patches installed with MBSA
 - <http://www.microsoft.com/technet/security/tools/mbsahome.msp>
- Install Windows XP SP2
- Enable Windows XP SP 2 Firewall

Defense



- Alternate browsers are known to help
 - Not supported by CIS
 - I use Firefox (www.mozilla.org/firefox)
- Test and secure IE with:
 - <http://browsercheck.qualys.com/>
- Install & Configure Anti-Virus Software
 - Update software & definitions as often as possible!

Defense



- Email tips:
 - View in plain text (prevents WMF vulnerability)
 - Don't open zip attachments without checking with sender
 - Upgrade to Outlook 2003, blocks images for you

Defense



- Not for everyone:
 - Disable NetBIOS Null Sessions
 - Disable Remote Registry Access
 - Disable insecure LANMAN passwords
 - Don't logon with administrator privileges *unless required*
 - Enable good account policies

Defense



- Guides to help you:
 - SANS Top Twenty Vulnerabilities
 - <http://www.sans.org/top20/>
 - Center for Internet Security standards
 - http://www.cisecurity.org/bench_win2000.html

Is my machine hacked?

- Popular question asked by all
- Free guides available from SANS (Windows & Linux)
 - www.sans.org/resources/winscheatsheet.pdf
 - www.sans.org/resources/linscheatsheet.pdf
- Use caution when using tools and techniques suggested



Scariest Article Of The Month

“U.S. Air Traffic Control Found Vulnerable”

<http://www.securityfocus.com/news/9729>

“...a government audit that found the systems insufficiently secured against cyber attacks.”



/* The End */

Questions? Comments? Flame Mail? Donations?

Paul_Asadoorian@brown.edu

This presentation:

<http://www.brown.edu/Research/SysAdmins/vuln-Oct-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>