

---

# Vulnerability Summary

## September 2003

Paul Asadoorian  
IT Security Specialist  
Brown University

---

# Vulnerabilities

---

- RPC DCOM (Again)
- Solaris sadmind root command execution
- Sendmail Buffer Overflow: Address Parsing
- OpenSSH – Multiple Vulnerabilities
- Internet Explorer: Multiple bugs

# RPC DCOM (Again)

---

- Another Buffer Overflow vulnerability in RPC DCOM (MS03-039)
- Heap overflow, harder to exploit
- So, what is RPC DCOM anyway?

# RPC DCOM (Again)

---

- “Remote Procedure Call – Distributed Component Object Model”
- Enables Software components to communicate across the network
- Allows code to execute remotely
- Uses many ports: 135-139, 445, 593
- Can be accessed over port 80 and 443 in certain environments

# RPC DCOM (Again)

---

- Proof-of-Concept code published
- Hackers working on multi-platform exploit
- Having trouble with the offset
- Wrong offset = crash (Segmentation Fault)

# RPC DCOM (Again)

---

- Defense
  - Patch, Patch, and More Patches
  - Block NetBIOS and other ports
  - Disable DCOM

# RPC DCOM (Again)

---

- The Analysis of RPC Long Filename Heap Overflow AND a Way to Write Universal Heap Overflow of Windows
  - <http://www.security.nnov.ru/search/document.asp?docid=5141>
- SANS Presentation on DCOM, Blaster, the blackouts, etc..
  - <http://isc.incidents.org/presentations/sansne2003.pdf>

# RPC DCOM (Again)

---

Its only a matter of time...

# Solaris sadmind root command execution

---

- Sadmind allows you to “*manage systems remotely, centralize configuration information, and monitor software usage.*”
- Distributed with the Solstice Management Suite
- Typically installed and enabled by default with Solaris SunOS 5.3 thru 5.9 (Solaris 2.x, 7, 8, 9)

# Solaris sadmind root command execution

---

- Uses weak authentication (AUTH\_SYS)
- Exploitable by sending RPC calls
- Tricks the server into executing commands as root
- Exploit is readily available (Published by HD Moore, <http://www.metasploit.com>)

# Solaris sadmind root command execution

---

- Defense
  - Block port 111 UDP and TCP
    - We block this on our border router
  - Enable stronger authentication (AUTH\_DES)
    - No Patch will be released!
    - See Sun Microsystems alert 56740
  - Turn off sadmind (/etc/inetd.conf)

# Solaris sadmind root command execution

---

- Instructions on how to configure sadmind properly
  - <http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56740>
- Security Advisory
  - <http://www.security.nnov.ru/search/document.asp?docid=5119>

# Sendmail Buffer Overflow: Address Parsing

---

- sendmail versions prior to 8.12.10
- Buffer Overflow – Execute arbitrary code by sending an email
- Exploit code exists for 8.11.6, certainly worth updating 😊

# Sendmail Buffer Overflow: Address Parsing

---

- Defense:
  - Apply patch for Sendmail 8.9.x through 8.12.9
  - Upgrade to 8.12.10
  - Disable Sendmail on machines where you don't need it
    - BAD: `/usr/lib/sendmail -bd -q`
    - GOOD: `/usr/lib/sendmail -q`

# Sendmail Buffer Overflow: Address Parsing

---

- CERT Advisory
  - <http://www.cert.org/advisories/CA-2003-25.html>
- Security.nnov.ru Advisory (Links to others)
  - <http://www.security.nnov.ru/search/news.asp?binid=2702>

# OpenSSH – Multiple Vulnerabilities

---

- OpenSSH prior to 3.7.1 contain a buffer overflow
- Heap Corruption when handling large packets
  - Remote shell access
- Actively being exploited

# OpenSSH – Multiple Vulnerabilities

---

- OpenSSH PAM challenge failure
  - OpenSSH 3.7.1p1 (portable)
  - Any platform
  - compiled with --with-pam
  - PrivilegeSeparation disabled
  - Protocol version 1 enabled (default)
  - ChallengeResponse enabled (default)
- Allows users to login with no password

# OpenSSH – Multiple Vulnerabilities

---

- Defense:
  - Upgrade to OpenSSH version 3.7.1p2
  - Always set “PermitRootLogin no”
  - Always set “Protocol 2”
  - Always set “UsePrivilegeSeparation yes”

# Internet Explorer: Multiple bugs

---

- Isn't there always?
- Currently 31 unpatched vulnerabilities
- Also 5 recognized by MS on 20-Aug-03

# Internet Explorer: Multiple bugs

---

- [VU#813208](#) Microsoft Internet Explorer does not properly render input type tag
  - DoS on client
- [VU#334928](#) Microsoft Internet Explorer contains buffer overflow in Type attribute of OBJECT element on double-byte character set systems
  - Execute Code on client computer

# Internet Explorer: Multiple bugs

---

- [VU#548964](#) Microsoft Windows BR549.DLL ActiveX control contains vulnerability
  - DoS and/or Execute Code on client computer
- [VU#865940](#) Microsoft Internet Explorer does not properly evaluate "application/hta" MIME type
  - Execute Code on client computer

# Internet Explorer: Multiple bugs

---

- [VU#205148](#) Microsoft Internet Explorer does not properly evaluate Content-Type and Content-Disposition headers
  - Read contents of Temporary Internet files
  - “execute arbitrary script with privileges of the user in the security context of the Local Machine Zone”

# Internet Explorer: Multiple bugs

---

- Defense:
  - Patch your browser (Windows Update)
  - Use another Browser:
    - Opera
    - Mozilla
  - Tweak Browser settings to disallow misbehaving web pages (ActiveX)
  - Run Host-Based IDS (They catch this stuff)

# Internet Explorer: Multiple bugs

---

- Unpatched IE Vulnerabilities
  - <http://www.pivx.com/larholm/unpatched/>
- Mozilla Project
  - <http://www.mozilla.org/>
- Opera
  - <http://www.opera.com/>
- Guides to securing IE:
  - <http://www.computerstuff.net/security/ieconfig.htm>
  - <http://www.sans.org/rr/paper.php?id=287>

# Web Site Blunder of the Month

---

Verisign SiteFinder

“Verisign Likes to Watch”

<http://www.theregister.co.uk/content/6/32926.html>

<http://siliconvalley.internet.com/news/article.php/3081611>

\*.com → Verisign

# /\* 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>