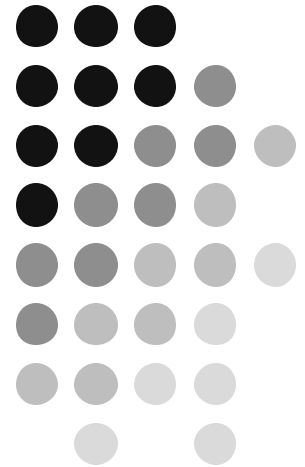


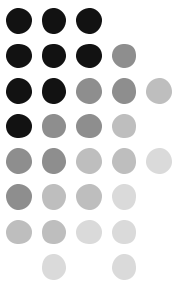
Vulnerability Summary

April 2003

Paul Asadoorian

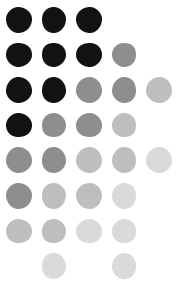
April 24, 2003





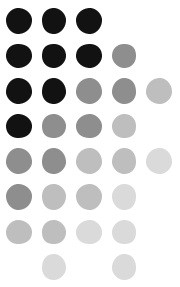
Terminology

- **Remote Exploit** – The ability to gain unauthorized access remotely, typically as root or an administrative account
- **Local Exploit** – The ability to escalate privileges from a non-root user to root level privileges (or equivalent, such as administrator)
- **MITM** (Man-In-The-Middle) – Placing yourself in between two hosts communicating on the network with malicious intent.
- **DoS** (Denial of Service) – Interrupt a network or hosts ability to function.
 - **DDoS** (Distributed Denial of Service) – Interrupts the network or host using many attacking hosts.



Vulnerabilities

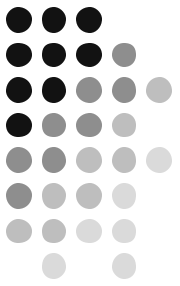
- Sendmail Remote Exploit (Again)
- Microsoft Terminal Services (RDP) MITM
- ptrace Linux Kernel Local Exploit
- Samba Remote Exploit
- Microsoft JVM Remote Exploit
- Microsoft Windows Kernel Contains Stack Overflow
- Paul's Pick of the Month
- Honorable Mentions



Sendmail Remote Exploit (Again)

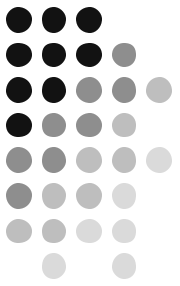
- All versions of Sendmail prior to 8.12.9
- Buffer overflow in the email address field (Attack comes in the form of an email)
- Allows for DoS and/or remote root exploit
- Exploit publicly available for Red Hat 7.3/7.2 and Slackware 8.0 with brute force feature
- Links:
 - <http://www.cert.org/advisories/CA-2003-12.html>
 - <http://www.kb.cert.org/vuls/id/897604>
 - <http://www.securityfocus.com/bid/7230/info/>
 - <http://www.security.nnov.ru/search/document.asp?docid=4311>

Sendmail Remote Exploit (Again)



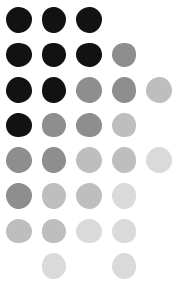
- Defense! Defense! Defense!
- Patch - <http://www.sendmail.org/8.12.9.html>
- Firewall – Block TCP port 25 incoming
 - Also gives you 100% SPAM blocking
- Host Intrusion Prevention -
 - Linux – Openwall (<http://www.openwall.com/>)
 - Linux – grsecurity (<http://www.grsecurity.net>)
 - Solaris – Disable Stack Execution (Very limited)
 - Solaris - Okena (<http://www.okena.com>)

Microsoft Terminal Services (RDP) MITM



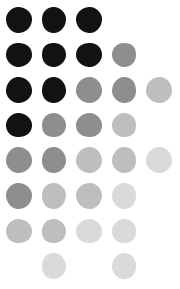
- Used for Remote Desktop access to Windows XP/2000, all are vulnerable
- No user key verification in the protocol (i.e. SSH asks you to accept the key, RDP does not)
- MS knows about the problem and is “investigating the feasibility in adding this functionality”
- Claims that exploit exists, but not released to the public
- Links:
 - <http://www.securityfocus.com/archive/1/317244/2003-03-29/2003-04-04/0>

Microsoft Terminal Services (RDP) MITM



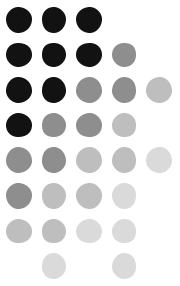
- Defense! Defense! Defense!
 - RDP over Stunnel (<http://www.stunnel.org/>)
 - RDP over IPSEC
 - Block TCP port 3389 incoming and/or outgoing
 - Use alternative:
 - Citrix ICA <http://www.citrix.com/>
 - VNC (Over SSH) <http://www.uk.research.att.com/vnc/>

ptrace Linux Kernel Local Exploit

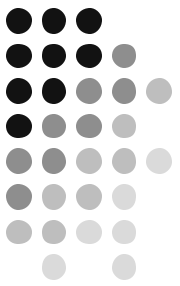


- Linux Kernel versions 2.2.18 and prior, as well as 2.4 kernels
- Allows local root, tested on Debian 3.0 unstable, kernel 2.4
- 'chmod 700 /proc' does NOT protect you from this vulnerability
- Links:
 - <http://www.kb.cert.org/vuls/id/176888>
 - <http://www.securityfocus.com/archive/1/171708>
 - <http://www.ciac.org/ciac/bulletins/l-076.shtml>
 - <http://www.securiteam.com/unixfocus/5FP0A2K9GQ.html>

ptrace Linux Kernel Local Exploit



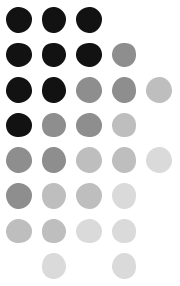
- Defense! Defense! Defense!
 - Patch – <http://www.kernel.org> (or vendor specific patches)
 - Watch what you users are doing, rule of least privilege
 - Host Intrusion Prevention (all ones mentioned before)
 - Linux Security Module <http://lsm.immunix.org/>



Samba Remote Exploit

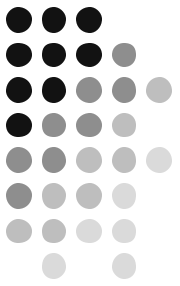
- Versions 2.2.8 and prior
- Remote root exploit, uses NetBIOS ports
- Working exploit circulating, tested on Debian 3.0 stable
- Links:
 - <http://www.kb.cert.org/vuls/id/267873>
 - <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0201>
 - <http://www.securityfocus.com/bid/7294>

Samba Remote Exploit



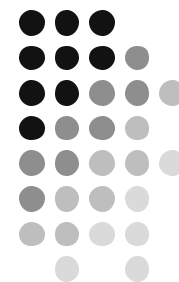
- Defense! Defense! Defense!
 - Patch – <http://www.samba.org/>
 - Block NetBIOS ports, already done for you at border
 - Host Intrusion Prevention (Previously mentioned)
 - Run Samba in a chroot environment?

Samba Remote Root Exploit



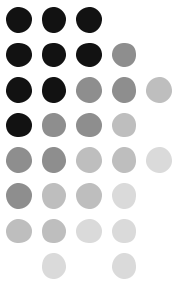
```
{ "samba-2.2.x - Debian 3.0 ", 0xbffffea2, linux_bindcode, 0 },
{ "samba-2.2.x - Gentoo 1.4.x ", 0xbfffe890, linux_bindcode, 0 },
{ "samba-2.2.x - Mandrake 8.x ", 0xbffff6a0, linux_bindcode, 0 },
{ "samba-2.2.x - Mandrake 9.0 ", 0xbfffe638, linux_bindcode, 0 },
{ "samba-2.2.x - Redhat 9.0 ", 0xbffff7cc, linux_bindcode, 0 },
{ "samba-2.2.x - Redhat 8.0 ", 0xbffff2f0, linux_bindcode, 0 },
{ "samba-2.2.x - Redhat 7.x ", 0xbffff310, linux_bindcode, 0 },
{ "samba-2.2.x - Redhat 6.x ", 0xbffff2f0, linux_bindcode, 0 },
{ "samba-2.2.x - Slackware 9.0 ", 0xbffff574, linux_bindcode, 0 },
{ "samba-2.2.x - Slackware 8.x ", 0xbffff574, linux_bindcode, 0 },
{ "samba-2.2.x - SuSE 7.x ", 0xbffffbe6, linux_bindcode, 0 },
{ "samba-2.2.x - SuSE 8.x ", 0xbffff8f8, linux_bindcode, 0 },
{ "samba-2.2.x - FreeBSD 5.0 ", 0xbfbff374, bsd_bindcode, 1 },
{ "samba-2.2.x - FreeBSD 4.x ", 0xbfbff374, bsd_bindcode, 1 },
{ "samba-2.2.x - NetBSD 1.6 ", 0xbfbfd5d0, bsd_bindcode, 1 },
{ "samba-2.2.x - NetBSD 1.5 ", 0xbfbfd520, bsd_bindcode, 1 },
{ "samba-2.2.x - OpenBSD 3.2 ", 0x00159198, bsd_bindcode, 2 },
{ "samba-2.2.8 - OpenBSD 3.2 (package)", 0x001dd258, bsd_bindcode, 2 },
{ "samba-2.2.7 - OpenBSD 3.2 (package)", 0x001d9230, bsd_bindcode, 2 },
{ "samba-2.2.5 - OpenBSD 3.2 (package)", 0x001d6170, bsd_bindcode, 2 },
{ "Crash (All platforms) ", 0xbade5dee, linux_bindcode, 0 },
```

Microsoft JVM Remote Exploit



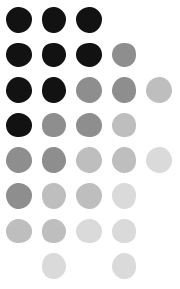
- All MS JVM versions prior to and including 5.0.3809
- Go to the command prompt and type “jview” to get version
- Must go to a web page with malicious applet
- Runs with permissions of user who is logged in
- Links:
 - <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-011.asp>
 - <http://www.securityfocus.com/bid/6221>
 - <http://www.kb.cert.org/vuls/id/447569>

Microsoft JVM Remote Exploit



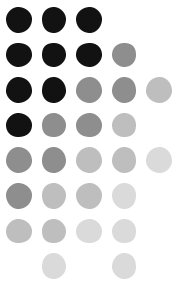
- Defense! Defense! Defense!
 - Run windows update
 - Use alternate browser for Java applet web site (Opera works well, <http://www.opera.com>)
 - Disable Java in Internet Explorer
 - Use application filtering to block Java applets (Netscreen has this ability)

Microsoft Windows kernel contains stack overflow



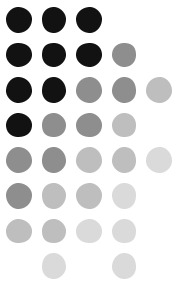
- Local Exploit, works on NT/2000/XP
- Patch is known to cause performance problems with Windows XP SP1
- Unchecked buffer in kernel that deals with message passing to the debugger
- Links:
 - <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-013.asp>
 - <http://www.kb.cert.org/vuls/id/446338>
 - <http://www.entercept.com/news/uspr/04-16-03.asp>

Microsoft Windows kernel contains stack overflow



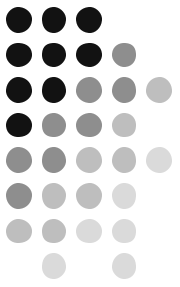
- Defense! Defense! Defense!
 - Apply Patch (Check bulletin for updates on the poor performance problem)
 - Host-Based Intrusion Detection/Prevention

Honorable Mentions



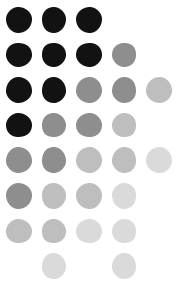
- Apache 2.x DoS
- Snort Preprocessor Remote Exploit
- MacOS X DirectoryService Privilege Escalation
- Multiple Vulnerabilities in Lotus Notes and Domino (Remote Exploit, DoS)
- Seti@Home Multiple Bugs (Remote Exploit)

Honorable Mentions: Favorite Web Site Hack-Of-The-Month



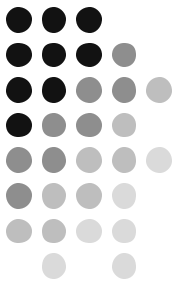
“Like a virgin - Madonna hacked
for the very first time”

<http://www.theregister.co.uk/content/6/30356.html>



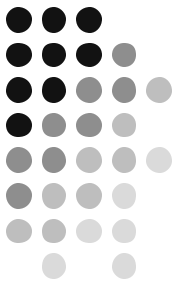
Paul's Pick of the Month

- Half Life Server DoS (Ver 3.1.1.0) Windows and Linux
- Sending a malformed packet to server causes it to crash
- Interrupts game play, causes server to use 100% of CPU
- Links:
 - <http://www.security.nnov.ru/search/document.asp?docid=4416>
 - <http://www.planethalflife.com/half-life/> (Not a security link, but an awesome resource for Half Life! Thanks Tom D.)



Paul's Pick of the Month

- Defense! Defense! Defense!
 - Don't run Half Life on your critical servers
 - Use WON-Authentication for your Half Life server
 - Block ports with firewall (Typically TCP 27015 and 28016)
 - Use Unreal Tournament 2003 instead 😊



Useful Links

- <http://www.security.nnov.ru>
- <http://www.securityfocus.com>
- <http://www.cert.org>
- <http://packetstormsecurity.nl/>
- <http://www.whitehats.com>