
Vulnerability Summary

September 2004



Paul Asadoorian
Lead IT Security Specialist
Brown University

Vulnerabilities

- MIT Kerberos Vulnerabilities
- Mozilla Vulnerabilities
- Apache Vulnerabilities
- WinZip Buffer Overflow Vulnerabilities
- Axis NetCam Bugs
- Netdetective: Part I – Finding Worms

MIT Kerberos Vulnerabilities

- Remote Code Execution and DoS Vulnerabilities
- All releases of Kerberos 5 up to and including krb5-1.3.4
- Appears to affect all platforms

MIT Kerberos Vulnerabilities

- Patches and upgrades available from Kerberos Homepage
 - <http://web.mit.edu/kerberos/>
- Latest version is krb5-1.3.5
- Caution: Cisco Systems VPN 3000's are vulnerable too
 - <http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml>

Mozilla Vulnerabilities

- Buffer overflows in:
 - E-mail VCards
 - Bitmap decoders
 - UTF-8 conversion
 - POP3 protocol handling
 - Send page feature
- Cross site scripting via link dragging

Mozilla Vulnerabilities

- Affected Products:
 - Mozilla 1.7
 - Mozilla Thunderbird 0.7
 - Mozilla Firefox 0.9
- New versions contain bug fixes and new features

Mozilla Vulnerabilities

- Upgrade now!
- Latest versions are:
 - Mozilla 1.7 .3
 - Mozilla Thunderbird 0.8
 - Mozilla Firefox 1.0PR (Pre-Release)
- New version of Firefox rocks!

Mozilla Vulnerabilities

- New Features Include:
 - Improved Pop-up blocker
 - Security Enhancements
 - Live Bookmarks (Very Cool!)
 - New Plug-in finder
 - Greatly Improved searching within web pages

Mozilla Vulnerabilities

- Mozilla project Homepage
 - <http://www.mozilla.org>
- Firefox Homepage
 - <http://www.mozilla.org/products/firefox/>
- “Switching from Internet Explorer to Mozilla Firefox”
 - <http://www.mozilla.org/products/firefox/switch.html>
- Advisory:
 - <http://www.security.nnov.ru/search/news.asp?binid=4020>

Apache Vulnerabilities

- Apache Version 2.0.x is vulnerable to buffer overflows and DoS
- Only Apache 2 series is vulnerable
- Overflow requires you supply it with a crafted .htaccess file

Apache Vulnerabilities

- Upgrade to Apache 2.0.51
- Run Apache in a chroot environment
- Turn off unused Apache features
 - Nessus finds many of these
 - TRACE & TRACK methods for example

Apache Vulnerabilities

- Apache Advisory:
 - <http://www.apache.org/dist/httpd/Announcement2.html>
- Security.nnov.ru Advisory:
 - <http://www.security.nnov.ru/search/news.asp?binid=4008>
- CERT Advisory:
 - <http://www.kb.cert.org/vuls/id/481998>

WinZip Buffer Overflow Vulnerabilities

- Buffer Overflow allows code execution
- Reported and found by vendor
- No other details available at this time
- How many users have this installed?

WinZip Buffer Overflow Vulnerabilities

- Winzip versions going back to 3.x appear to be vulnerable
- Upgrade to 9.0 SR-1:
 - <http://www.winzip.com/upgrade.htm>
- Use alternative, such as ZipCentral:
 - <http://zipcentral.iscool.net/>

Axis NetCam Bugs

- Obtain /etc/passwd file
- Create your own administrator account
- Hardcoded backdoor username and password

Axis NetCam Bugs

- Shell script points at cam and adds admin password
- User: wh00t / Password: wh00t
- Firmware updates available, but appear to fix completely different bugs?

Axis NetCam Bugs

- Proof-Of-Concept code available
- Many Axis netcams online, use your GoogleVision
- Beer Mate?
 - <http://203.217.10.160/view/indexFrame.shtml>

Axis NetCam Bugs

- Axis NetCams can be easily found using Google (hence the term GoogleVision)
- See the “Jonny – I Hack stuff” web site:
 - <http://johnny.ihackstuff.com/index.php?module=prodreviews>

Axis NetCam Bugs

- Upgrade to latest versions, fixes some problems
 - <http://www.security.nnov.ru/search/document.asp?docid=6780>
- Restrict access to your cameras or they will be part of Googlevision



Netdetective: Part I - Finding Worms

- Worm traffic can be easily identified
- 20+ hosts scanning for port 445 stands out
- Can infect machines quite rapidly
- Leads to network destruction

Netdetective: Part I - Finding Worms

- How do you find these hosts easily?
- How do you verify they are in fact infected?
- How do you process them quickly and efficiently?

Netdetective: Part I - Finding Worms

- Worm behavior:
 - Scan for vulnerabilities on port 445
 - Scans on both local and remote subnets
 - Communicate to “Botnet” on port 6667
 - They all listen on a high port number for FTP
- This seems to be pretty standard

Netdetective: Part I - Finding Worms

- Use a packet sniffer (tcpdump) to find all outgoing scan traffic:

```
tcpdump -c 100 -i eth1 -nn  
src net MY.SUBNET.0.0/16 \  
and dst port 445 \  
or port 6667 or port 7000
```

Netdetective: Part I - Finding Worms

- Connect to all ports and grab the banner:

```
amap -U -q -B <IP Address> 1-65535
```

- The following banner is bad:

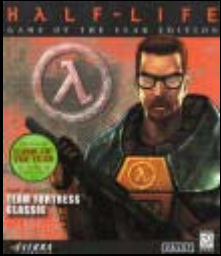
```
Banner on 128.148.55.195:16711/tcp :  
220 Bot Server (Win32)\r\n
```

Netdetective: Part I - Finding Worms

- Email the results to Network people
- Compromised hosts get filtered
- Tracking tickets get created

Netdetective: Part I - Finding Worms

- Script called “Wormreport” (how original) automates the whole process
- We run it hourly
 - Only one copy runs at a time
 - It “pings” hosts first before testing
- Download here
 - <http://www.brown.edu/Research/SysAdmins/wormreport.sh.txt>



Fragger Warning

- Buffer overflow in numerous games, including:
 - Half Life
 - Unreal tournament 2004
 - Halo
- Allows remote code execution
- Upgrade and patch your games (Unreal Tournament 2004 has patch)

Article Of The Month

“Sasser author gets IT security job”

http://www.theregister.co.uk/2004/09/20/sasser_kiddo_offered_job/

“He's been offered work as a trainee software developer working on security products, such as firewalls, even though he may go to prison for creating one of the most destructive computer viruses to date.”

/* The End */

Questions? Comments? Flame Mail?

Paul_Asadoorian@brown.edu

This presentation:

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