
Vulnerability Summary

March 2004

Paul Asadoorian
IT Security Specialist
Brown University

Vulnerabilities

- Microsoft Outlook shell characters problem
- Multiple Vulnerabilities in OpenSSL
- Multiple ISS Products Heap Overflow
- dtlogin remote root
- Hacking Printers: Part I

Microsoft Outlook shell characters problem

- Affected Software
 - Microsoft Office XP Service Pack 2
 - Microsoft Outlook 2002 Service Pack 2
- Incorrect interpretation of the [mailto:](#) tag in HTML email
- Leads to code being executed in “Local Machine” context
 - This is very bad

Microsoft Outlook shell characters problem

- Defense
 - Apply patches
 - Numerous problems
 - Weird dialog box
 - Patch not applying
 - See Help Desk/Desktop services for details

Microsoft Outlook shell characters problem

- Links

- <http://security.nnov.ru/search/news.asp?binid=3512>
- <http://www.idefense.com/application/poi/display?id=79&type=vulnerabilities&flashstatus=true>
- <http://microsoft.com/technet/security/bulletin/MS04-009.msp>

Multiple Vulnerabilities in OpenSSL

- OpenSSL versions before 0.9.7d or 0.9.6m are vulnerable
- Three different bugs could causes a DoS condition in each case
- Vulnerability Note VU#465542 affects numerous vendor implementations
 - See <http://www.kb.cert.org/vuls/id/465542> for details

Multiple Vulnerabilities in OpenSSL

- Defense
 - Upgrade to OpenSSL versions 0.9.7d or 0.9.6m
 - Apply patches from your vendor
 - Cisco IOS upgrades are available in April

Multiple Vulnerabilities in OpenSSL

- <http://security.nnov.ru/search/news.asp?binid=3532>
- <http://www.us-cert.gov/cas/techalerts/TA04-078A.html>
 - <http://www.kb.cert.org/vuls/id/288574>
 - <http://www.kb.cert.org/vuls/id/484726>
 - <http://www.kb.cert.org/vuls/id/465542>

Multiple ISS Products Heap Overflow

- Buffer overflow in handling of ICQ alerts
- Can be exploited with a single spoofed packet
 - Easily done with the echo service
- Witty worm uses this vulnerability to propagate

Multiple ISS Products Heap Overflow

- RealSecure Network and Server Sensor
- Proventia Series XPU
- RealSecure Desktop
- RealSecure Guard
- RealSecure Sentry
- BlackICE Agent
- BlackICE PC Protection
- BlackICE Server Protection

Multiple ISS Products Heap Overflow

- Defense
- Upgrade to latest versions of ISS products (See advisory link)
- Witty worm
 - Reboot removes the worm
 - May cause hard drive failure (overwrites MBR)

Multiple ISS Products Heap Overflow

- <http://security.nnov.ru/search/news.asp?binid=3534>
- <http://isc.sans.org/diary.html?date=2004-03-20> – Witty worm write-up
- <http://xforce.iss.net/xforce/alerts/id/166> - ISS advisory
- <http://www.eeye.com/html/Research/Advisories/AD20040226.html>

dtlogin remote root

- Buffer overflow in the dtlogin process
- Leads to “execute arbitrary code, read sensitive information, or cause a denial of service”
- Remote root possible
 - Listens on UDP port 177

dtlogin remote root

- Defense
- No vendors have released patches (according to Cert)
- Block UDP port 177
- On a SunOS 5.8 system:

```
/usr/dt/config/Xconfig  
  
# To disable listening for XDMCP requests from X-terminals.  
#  
Dtlogin.requestPort:      0
```

dtlogin remote root

- <http://www.kb.cert.org/vuls/id/179804>
- <http://security.nnov.ru/search/news.asp?binid=3543>

Hacking Printers: Part I

- Determining firmware revision
- Find vulnerabilities associated with the firmware
 - We'll cover just one
- Fixing vulnerability
 - This is what makes the hat white instead of black 😊

Hacking Printers: Part I

- SNMP and default community strings
- Default strings are “public” and “internal”
- Allows you to read the entire “MIB” tree
 - All information available via SNMP
 - Includes route and MAC tables
 - In some firmware includes device password in hex

Hacking Printers: Part I

- Newer firmware allows you to fix the SNMP problem
- Commands exist to disable the default community strings
- But how do I know the firmware revision of all printers on the network?

Hacking Printers: Part I

- Use the hack to fix the hack
- New hack, er vulnerability testing, tool “printerwalk.sh”
- Grabs the IP address and sysDescr MIB using the default community strings
- Also useful to grab entire tree

Hacking Printers: Part I

- printerwalk.sh

```
# ./printerwalk.sh
```

```
Error: Please specify a Community String and an IP Subnet  
(nnn.nnn.nnn) .
```

```
printerwalk.sh <Community String> <Subnet> [desc|all]
```

```
By default printerwalk will grab just the description MIB  
(sysDescr.0)
```

Hacking Printers: Part I

- Ready, aim...

```
# ./printerwalk.sh public MY.SUB.NET desc > MY.SUB.NET.out
```

Hacking Printers: Part I

- Results

```
* IPAddress: MY.SUB.NET.113
SNMPv2-MIB::sysDescr.0 = STRING: HP ETHERNET MULTI-
ENVIRONMENT,ROM A.05.03,JETDIRECT,JD24, EEPROM A.08.32
```

Hacking Printers: Part I

- To fix the problem we need to:
 1. Upgrade the firmware
 2. Apply the config change

Hacking Printers: Part I

- Upgrade the firmware using HP WebJetAdmin
- Download from:
 - <http://www.hp.com/go/webjetadmin>
- More detailed instructions to follow in the future

Hacking Printers: Part I

- Now telnet to the printer (I know, I know)
- View the config
- Note version number and default community setting

```
Please type "?" for HELP, or "/" for
current settings
> /

===JetDirect Telnet Configuration===
  Firmware Rev.      : E.08.49
  MAC Address       : XX:XX:XX:XX:XX:XX
  Config By        : DHCP

  IP Address        : MY.SUB.NET.117
  Subnet Mask       : 255.255.255.0
  Default Gateway   : MY.SUB.NET.1
  Syslog Server     : Not Specified
  Idle Timeout      : 90 Seconds
  Set Cmnty Name    : *****
  Host Name         : HACKME
  Default Get Cmnty : Enabled

  DHCP Config      : Enabled
  Passwd           : Enabled
  IPX/SPX          : Disabled
  DLC/LLC          : Enabled
  Ethertalk        : Disabled
  Banner page      : Disabled
```

Hacking Printers: Part I

- Disable default community
- “Quit” which is really save and quit

```
> default-get-cmnty: 0
> quit

===JetDirect Parameters Configured===

      IP Address       : MY.SUB.NET.117
      Subnet Mask     : 255.255.255.0
      Default Gateway : MY.SUB.NET.1
      Syslog Server    : Not Specified
      Idle Timeout    : 90 Seconds
      Set Cmnty Name   : *****
      Host Name        : HACKME
      Default Get Cmnty : Disabled

      DHCP Config     : Enabled
      Passwd           : Enabled
      IPX/SPX          : Disabled
      DLC/LLC          : Enabled
      Ethertalk        : Disabled
      Banner page      : Disabled

User Quitting
```

Hacking Printers: Part I

- HP WebJetAdmin uses SNMP to collect information about the printer
 - Changing this will decrease functionality
- Also uses it during the firmware upgrade process
- The write string is different and can be changed through WebJetAdmin
 - Make it different than the device password

Website Of The Month

“Googledorks”

<http://johnny.ihackstuff.com/index.php?module=prodreviews>

googleDork noun 1. Slang. An inept or foolish person as revealed by Google.

/* 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/>