COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK
PRINT ME IF YOU Dare
Firmware Update Attack and the Rise of Printer Malware

Ang Cui | Sal Stolfo
{ang|sal}@cs.columbia.edu
Columbia University Intrusion Detection Systems Lab

Update: 12.23.2011 HPSBPI02728 SSRT100692 rev.2
### Vendors

<table>
<thead>
<tr>
<th>Vendors</th>
<th>2Q10 Unit Shipments</th>
<th>2Q10 Market Share</th>
<th>2Q09 Unit Shipments</th>
<th>2Q09 Market Share</th>
<th>2Q10/2Q09 Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. HP</td>
<td>11,934,950</td>
<td>41.0%</td>
<td>9,757,118</td>
<td>40.2%</td>
<td>22.3%</td>
</tr>
<tr>
<td>2. Canon</td>
<td>5,608,371</td>
<td>19.3%</td>
<td>4,942,090</td>
<td>20.4%</td>
<td>13.5%</td>
</tr>
<tr>
<td>3. Epson</td>
<td>4,083,638</td>
<td>14.0%</td>
<td>3,399,607</td>
<td>14.0%</td>
<td>20.1%</td>
</tr>
<tr>
<td>4. Samsung</td>
<td>1,667,671</td>
<td>5.7%</td>
<td>1,094,660</td>
<td>4.5%</td>
<td>52.3%</td>
</tr>
<tr>
<td>5. Brother</td>
<td>1,553,425</td>
<td>5.3%</td>
<td>1,319,257</td>
<td>5.4%</td>
<td>17.7%</td>
</tr>
<tr>
<td>Others</td>
<td>4,247,879</td>
<td>14.6%</td>
<td>3,731,497</td>
<td>15.4%</td>
<td>13.8%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>29,095,934</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>24,244,229</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>20.0%</strong></td>
</tr>
</tbody>
</table>

Source: IDC Worldwide Quarterly Hardcopy Peripherals Tracker, August 2010

---

**When in doubt, follow the $$$**

**HP IPG: 41% Market Share, Ships 40M units per year!**
23. Are current HP multifunction printers susceptible to viruses and worms?
No, since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. HP MFPs use non-standard operating systems other than Windows. Consequently, they are immune to these viruses and worms. In practice, there have been no known instances of viruses or worms infecting HP MFPs.

In the future HP will likely ship MFPs which include an embedded version of the Windows operating system. However, there are a number of practical reasons why this won’t increase the security risk faced by customers.

24. Does this mean that HP MFPs are completely safe from worms and viruses?
No, since it is technically possible for someone to craft a virus or worm that targets the non-standard operating systems shipped with the MFPs. However, HP considers the probability of such an event to be considerably lower. Hackers are more likely to be interested in exploiting vulnerabilities in workstations and servers since they are more widespread and require less expertise.

THANKS!

Jatin Kataria

Sal Stolfo

Jon Voris
INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”

MSNBC
INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica
INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica

“Hackers could turn your printer into a flaming death bomb”
Gawker
Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware

Internet News Machine... (Day 1)

“Millions of printers open to devastating hack attack, researchers say”
MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
ars technica

“Hackers could turn your printer into a flaming death bomb”
Gawker

“Can hackers really use your HP printer to steal your identity”
INTERNET NEWS MACHINE... (DAY 1)

“Millions of printers open to devastating hack attack, researchers say”
  MSNBC

“HP printers can be remotely controlled and set on fire, researchers claim”
  ars technica

“Hackers could turn your printer into a flaming death bomb”
  Gawker

“Can hackers really use your HP printer to steal your identity and blow up your house?”
  gizmodo
Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware

Internet News Machine... (Day 2, Smack Down and Spanking!)

“HP refutes reports that can be remotely set on fire”
   FoxNews

“Hackers can set your house on fire through your older LaserJet printer”
   Hitechnology.com

“HP smacks down Columbia University printer fire report”
   silobreaker

“HP douses fiery printer hack theory”
   Business Recorder

“HP memo spanks Columbia researchers over flaming printers flap”
   Allthingsd.com
“HP hit with lawsuit over flaming-printer hack”
INTERNET NEWS MACHINE... (MY FAVORITE)

“HP HIT WITH LAWSUIT OVER FLAMING-PRINTER HACK”

Wired!
INTERNET NEWS MACHINE... THE NOT TERRIBLE

"SECURITY FLAW IN PRINTERS COULD EXPOSE BUSINESSES TO HACKERS"
HUFFINGTONPOST

"COULD YOUR PRINTER BE A TROJAN HORSE? RESEARCHERS SAY YES!"
CNET

"COLUMBIA RESEARCHERS SHOW REMOTE HP PRINTER HIJACK"
BETANews
Disclosure: November 21st

Firmware Release: December 23rd

Printer Firmwares Have Been Updated

2005 - 2011
**Print Me If You Dare**

**Firmware Update Attack and the Rise of Printer Malware**

Based on my disclosure, these printer firmwares have been updated:

<table>
<thead>
<tr>
<th>HP LaserJet Enterprise 500 color M551</th>
<th>HP LaserJet P4014</th>
<th>HP LaserJet M9040 Multifunction Printer</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP LaserJet Enterprise 600 M601</td>
<td>HP LaserJet P4015</td>
<td>HP LaserJet 9050</td>
</tr>
<tr>
<td>HP LaserJet Enterprise 600 M602</td>
<td>HP LaserJet 4240</td>
<td>HP LaserJet M9050 Multifunction Printer</td>
</tr>
<tr>
<td>HP LaserJet Enterprise 600 M603</td>
<td>HP LaserJet 4250</td>
<td>HP 9200c Digital Sender</td>
</tr>
<tr>
<td>HP Color LaserJet CM1312 Multifunction</td>
<td>HP LaserJet 4345 Multifunction Printer</td>
<td>HP 9250c Digital Sender</td>
</tr>
<tr>
<td>HP LaserJet Pro CM1415 Color Multifunction</td>
<td>HP LaserJet 4350</td>
<td>HP Color LaserJet 9500</td>
</tr>
<tr>
<td>HP Color LaserJet CP1510</td>
<td>HP LaserJet P4515</td>
<td>HP Color LaserJet CM3530</td>
</tr>
<tr>
<td>HP LaserJet M1522 Multifunction Printer</td>
<td>HP Color LaserJet Enterprise CP4520</td>
<td>HP Color LaserJet 3800</td>
</tr>
<tr>
<td>HP LaserJet Pro CP1525 Color Printer</td>
<td>HP Color LaserJet Enterprise CP4525</td>
<td>HP Color LaserJet CP4005</td>
</tr>
<tr>
<td>HP LaserJet Pro M1536 Multifunction Printer</td>
<td>HP Color LaserJet Enterprise CM4540</td>
<td>HP Color LaserJet CM6040</td>
</tr>
<tr>
<td>HP Color LaserJet CP2025</td>
<td>HP LaserJet Enterprise M4555 Multifunction</td>
<td>HP CM8060 Color Multifunction Printer</td>
</tr>
<tr>
<td>HP LaserJet P2035</td>
<td>HP Color LaserJet 4700</td>
<td>HP LaserJet 9040</td>
</tr>
<tr>
<td>HP LaserJet P2055</td>
<td>HP Color LaserJet 4730 Multifunction Printer</td>
<td>HP LaserJet M3027 Multifunction Printer</td>
</tr>
<tr>
<td>HP Color LaserJet 3000</td>
<td>HP LaserJet M5035</td>
<td>HP Color LaserJet CP3525</td>
</tr>
<tr>
<td>HP LaserJet P3005</td>
<td>HP LaserJet 5200n</td>
<td>HP Color LaserJet CP5525</td>
</tr>
<tr>
<td>HP LaserJet Enterprise P3015</td>
<td>HP Color LaserJet Professional CP5225</td>
<td>HP Color LaserJet 5550</td>
</tr>
<tr>
<td>HP Color LaserJet CP6015</td>
<td>HP Color LaserJet CM6030</td>
<td></td>
</tr>
</tbody>
</table>

**CVE:** CVE-2011-4161

**SSRT:** 100692 rev.2

---

**Columbia University**

**In the City of New York**

---

28c3/12.29.2011
Research in Context. Who am I? Why am I doing this?

4th Year Ph.D. Candidate
Intrusion Detection Systems Lab
Columbia University
Research In Context. Who am I? Why am I doing this?

Past Publications:

- Pervasive Insecurity of Embedded Network Devices. [RAID10]
- A Quantitative Analysis of the Insecurity of Embedded Network Devices. [ACSAC10]
- Killing the Myth of Cisco IOS Diversity: Towards Reliable Large-Scale Exploitation of Cisco IOS. [USENIX WOOT 11]
- Defending Legacy Embedded Systems with Software Symbiotes. [RAID11]
- From Prey to Hunter: Transforming Legacy Embedded Devices Into Exploitation Sensor Grids. [ACSAC11]
Research In Context. Previous work studying **Embedded Insecurity**

**Vulnerable Embedded System Scanner**

**Embedded Exploitation**
Research In Context. Previous work studying Embedded Insecurity

Vulnerable Embedded System Scanner

Continuously Monitoring Internet for Trivially Vulnerable Embedded Devices
Research In Context. Previous Work Studying Embedded Insecurity

Vulnerable Embedded System Scanner

Continuously Monitoring Internet for Trivially Vulnerable Embedded Devices

1.4 Million Embedded Devices on the Internet with Default Passwords!
Research In Context. Previous Work Studying Embedded Insecurity

Vulnerable Embedded System Scanner

Continuously Monitoring Internet for Trivially Vulnerable Embedded Devices

1.4 Million Embedded Devices on the Internet with Default Passwords!

75,000 Vulnerable HP Printers on the internet. (We’ll get back to this)
Embedded Exploitation: Bidirectional Approach

Top Down: Internet Substrate:

Bottom Up: Common Embedded Devices:
Embedded Exploitation: Bidirectional Approach

Top Down: Internet Substrate: Routers (Blackhat 2011)

Bottom Up: Common Embedded Devices: Printers (now)
Can Embedded Systems Be Exploited?
HAVE EMBEDDED SYSTEMS BEEN EXPLOITED?
HAVE **YOUR** EMBEDDED SYSTEMS **B E E N  E X P L O I T E D**?
Have **Your** Embedded Systems **B e e n  E x p l o i t e d**?

How do you know for **s**ure?
Your router/printer has been owned 3d

Can you really remove the malware?
LET'S TALK
HP Koan: How does printer update firmware?...
HP Koan: How does printer update firmware?... PRINT!

HP LaserJet Printer and Multifunction Printer (MFP) series - Performing a Firmware Upgrade

Remote firmware update
Determining the current level of firmware
Downloading the latest firmware from www.hp.com
What you should know before downloading firmware to the printer or Multifunction Printer (MFP)
Remote firmware update using FTP through a browser
Remote firmware update using FTP on a direct network connection (Microsoft Windows)
For Shared Windows Systems
Using USB
Updating firmware using "HP Easy Firmware Upgrade" utility
Remote firmware update using the LPR command
Remote firmware update using the HP Printer Utility (Macintosh OS X)
Remote firmware update using FTP on a direct network connection (Macintosh)
Remote firmware update using HP Web JetAdmin
Remote firmware update for UNIX systems
Printer messages during the firmware update
Troubleshooting a firmware update

From “HP LaserJet Printer and Multifunction Printer (MFP) series - Performing a Firmware Upgrade”
HP Koan: How does printer update firmware?... PRINT!

Remote firmware update using the LPR command


Complete the following steps to update the firmware by using the LPR command.

1. Type `lpr -P -S -o l -or- lpr -S -Pbinps`, where can be either the TCP/IP address or the hostname of the product, and where is the filename of the .RFU file from a command window.

   NOTE: The parameter (-o l) consists of a lowercase "O", not a zero, and a lowercase "L", not a numeral 1. This parameter sets the transport protocol to binary mode.

2. Press `Enter` on the keyboard. The messages described in the section "Printer messages during the firmware update" appear on the control panel.

   NOTE: The product automatically restarts the firmware to activate the update. At the end of the update process, the Ready message appears on the control panel.

3. Type exit at the command prompt to close the command window.
You see where this is going...
PRINT ME IF YOU DARE
FIRMWARE UPDATE ATTACK AND THE RISE OF PRINTER MALWARE

LET'S PLAY... STARE AT BINARY BLOB FTW

HP RFU (REMOTE FIRMWARE UPDATE) FILE

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

28C3/12.29.2011
HP RFU (Remote Firmware Update) file

- PJL Command (Printer Job Language)
HP RFU (Remote Firmware Update) file

- PJL Command
- A SINGLE PJL Command
HP RFU (Remote Firmware Update) file

- PJL Command
- A single PJL Command
- A single PJL Command with 7MB of data
HP RFU (Remote Firmware Update) file

- PJL Command
- A single PJL Command
- A single PJL Command with 7MB of data
- A single PJL Command with 7MB of Compressed (not encrypted) Data
HP RFU (Remote Firmware Update) file

- PJL Command
- A single PJL Command
- A single PJL Command with 7MB of data
- A single PJL Command with 7MB of Compressed (not encrypted) Data
- Data is integrity checked, but is it SIGNED?
So DO HP RFUs use digital signature?

<table>
<thead>
<tr>
<th>CODE CRC ERROR SEND FULL RFU ON PORT</th>
<th>An error occurred during a firmware upgrade.</th>
<th>Contact an HP-authorized service or support provider.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORRUPT FIRMWARE IN EXTERNAL ACCESSORY</td>
<td>The product detected corrupt firmware in an input or output accessory.</td>
<td>Upgrade the firmware. Printing can continue, but jams might occur.</td>
</tr>
<tr>
<td>For help press ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA RECEIVED</td>
<td>The product is waiting for the command to print (such as waiting for a form feed, or when</td>
<td>Press ox to continue.</td>
</tr>
<tr>
<td>To print last page</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Look through error messages… Code CRC != Signature
Stating the obvious:

- LPR / RAW Printing has no authentication mechanism
Stating the obvious:

- **LPR / RAW Printing has no authentication mechanism**
- **PJL can be embedded in Postscript (and lots else)**
Stating the obvious:

- LPR / RAW Printing has no authentication mechanism
- PJL can be embedded in Postscript (and lots else)
- Malicious RFU = Printer malware
STATING THE OBVIOUS:

• LPR / RAW PRINTING HAS NO AUTHENTICATION MECHANISM
• PJL CAN BE EMBEDDED IN POSTSCRIPT (AND LOTS ELSE)

• MALICIOUS RFU = PRINTER MALWARE
• MALICIOUS RFU + DOC FORMAT ATTACK VECTOR

= SELF-PROPAGATING PRINTER MALWARE, EMBEDDED SPEAR-PHISHING, ETC
Next step: Reverse RFU format
Next step: Reverse RFU format

What didn’t work:

- Staring at binary blob
- Binwalk
- Common FS headers
- Googling
- Asking HP, Friends, Adviser, etc
Bricking the printer is pretty easy…

Unbricking the printer is also easy. Hmmm…
Bricking the printer is pretty easy...

Unbricking the printer is also easy. Hmmm...

Idea: Extract boot code, reverse RFU parser
Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware

2055 Printer Design
NO FIRE. SRSLY GOIS! MKAY?
Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware

NIC Controller

BOOT "ROM"

Memory

Persistent Storage

Formatter Board

Engine Controller Board
Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware

- Marvell 88E11118 ARM SoC
- Spansion FL064P
- ELPIDA E1116AL

Marvell 88PA2AL2-TAH1 ARM SoC

- Marvel GigE Transceiver
- Spansion SPI “ROM”
  - 64Mbit Flash Chip
- 128MB DDR2 SDRAM
- ARM SoC (NDA!)
2055DN Formatter Board

Main SoC Boots from SPI-Flash

Marvell SoC (no data sheet)

SPANSON FLASH (have datasheet!)
## PRINT ME IF YOU DARE
### Firmware Update Attack and the Rise of Printer Malware

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>One Byte Command Code</th>
<th>Description</th>
<th>Address Bytes</th>
<th>Mode Bit Cycle</th>
<th>Dummy Bytes</th>
<th>Data Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>READ</td>
<td>(03h) 0000 0011</td>
<td>Read Data bytes</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>FAST_READ</td>
<td>(0Bh) 0000 1011</td>
<td>Read Data bytes at Fast Speed</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>DOR</td>
<td>(3Bh) 0011 1011</td>
<td>Dual Output Read</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>QOR</td>
<td>(6Bh) 0110 1011</td>
<td>Quad Output Read</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>DIOR</td>
<td>(BBh) 1011 1011</td>
<td>Dual I/O High Performance Read</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>QIOR</td>
<td>(EBh) 1110 1011</td>
<td>Quad I/O High Performance Read</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>RDID</td>
<td>(9Fh) 1001 1111</td>
<td>Read Identification</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to 81</td>
</tr>
<tr>
<td></td>
<td>READ_ID</td>
<td>(90h) 1001 0000</td>
<td>Read Manufacturer and Device Identification</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>Write Control</td>
<td>WREN</td>
<td>(06h) 0000 0110</td>
<td>Write Enable</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>WRDI</td>
<td>(04h) 0000 0100</td>
<td>Write Disable</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Erase</td>
<td>P4E</td>
<td>(20h) 0010 0000</td>
<td>4 KB Parameter Sector Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>P8E</td>
<td>(40h) 0100 0000</td>
<td>8 KB (two 4 KB) Parameter Sector Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>(DDh) 1101 1000</td>
<td>64 KB Sector Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>BE</td>
<td>(60h) 0110 0000 or</td>
<td>Bulk Erase</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(C7h) 1100 0111</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program</td>
<td>PP</td>
<td>(02h) 0000 0010</td>
<td>Page Programming</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to 256</td>
</tr>
<tr>
<td></td>
<td>QPP</td>
<td>(32h) 0011 0010</td>
<td>Quad Page Programming</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to 256</td>
</tr>
<tr>
<td>Status &amp; Configuration Register</td>
<td>RDSR</td>
<td>(09h) 0000 0101</td>
<td>Read Status Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>WRR</td>
<td>(01h) 0000 0001</td>
<td>Write (Status &amp; Configuration) Registers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to 2</td>
</tr>
<tr>
<td></td>
<td>RCR</td>
<td>(35h) 0011 0011</td>
<td>Read Configuration Register (CFG)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td></td>
<td>CLSR</td>
<td>(30h) 0011 0000</td>
<td>Reset the Erase and Program Flag (SR5 and SR6) and restore normal operation</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Power Saving</td>
<td>DP</td>
<td>(B9h) 1011 1001</td>
<td>Deep Power-Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>RES</td>
<td>(ABh) 1010 1011</td>
<td>Release from Deep Power-Down Mode</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ABh) 1010 1011</td>
<td>Release from Deep Power-Down and Read Electronic Signature</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>OTP</td>
<td>OTPP</td>
<td>(42h) 0100 0010</td>
<td>Programs one byte of data in OTP memory space</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>OTPR</td>
<td>(4Bh) 0100 1011</td>
<td>Read data in the OTP memory space</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
</tbody>
</table>
ATTEMPT ONE:

- **Arduino SPI Dumper**
  - 40 lines of AVR code
  - Small python controller program
- **Monkey soldering**
ATTEMPT ONE:

- **Arduino SPI Dumper**
  - 40 lines of AVR code
  - Small Python controller program
- **Monkey soldering**
ATTEMPT ONE:

- **ARDUINO SPI DUMPER**
  - 40 LINES OF AVR CODE
  - SMALL PYTHON CONTROLLER PROGRAM
- MONKEY SOLDERING

- **GRADE: B-**
  - (WORKED, BUT POORLY)
ATTEMPT TWO:

- **Arduino SPI Dumper**
  - 40 lines of AVR code
  - Small Python controller program
- **Monkey soldering**
- **Duct-tape**
- **Grade: A+**
# SPI"ROM" Dump

<table>
<thead>
<tr>
<th>Address</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000002A</td>
<td>Start Image. Entry @ %#x\r\n</td>
</tr>
<tr>
<td>00000029</td>
<td>FAIL: imageTableIndex = %d\r\n</td>
</tr>
<tr>
<td>0000001D</td>
<td>Cannot start SPI ROM image\r\n</td>
</tr>
<tr>
<td>00000111</td>
<td>&lt;= BootSPIROM \r\n</td>
</tr>
<tr>
<td>00000011</td>
<td>=&gt; BootEEPROM \r\n</td>
</tr>
<tr>
<td>00000033</td>
<td>BootEEPROM: failed to read image size &amp; checksum\r\n</td>
</tr>
<tr>
<td>0000002D</td>
<td>BootEEPROM: imageSize = %d, checkSum = %#x\r\n</td>
</tr>
<tr>
<td>0000002F</td>
<td>BootEEPROM: failed to read image from EEPROM\r\n</td>
</tr>
<tr>
<td>00000039</td>
<td>BootEEPROM: invalid checksum. Should be: %#x, is: %#x\r\n</td>
</tr>
<tr>
<td>0000001C</td>
<td>Cannot start EEPROM image\r\n</td>
</tr>
<tr>
<td>000000B</td>
<td>BOOTCODE\r\n</td>
</tr>
<tr>
<td>0000042</td>
<td>FLASH 0x%x=0x%x bytes * 0x%x sectors (%x bootcode, %x reserved)\r\n</td>
</tr>
</tbody>
</table>

## Boot SPI-ROM Findings:

- **Not ROM (flash)**
- **8MB capacity**
- **Small Boot-Loader**
- **Factory Reset RFU Image (<1 MB)**
- **RFU Parser in boot-loader**
SPI"ROM" Dump

Notice the “UAT” header
Where have I seen this before?
HP RFU (Remote Firmware Update) file

Let's play... Stare at binary blob FTW
BootSPIRom: reads image size and checksum
Let’s stare at binary blob FTW

7929906 = 0x790032H

Shift for alignment

Hrm....

BootSPIRom: reads image size and checksum
Let's stare at binary blob FTW

7929906  
=  
0x790032H

0x32 bytes header  
Payload starts with  
"0xAA554154"

Shift again  
For alignment

BOOTSPIRom: reads image size and checksum
Let's stare at binary blob FTW

000000 00 AC 00 0F 00 03 F7 67 00 00 00 00 00 79 00 00 AA 55
000012 41 54 00 00 01 20 00 67 C6 8C 00 E5 89 A8 00 00 08 00
000024 00 67 C7 AC 00 00 20 E0 00 00 4D 3C 00 67 E8 8C 00 00
000036 21 86 00 00 50 91 00 68 08 12 00 00 20 28 00 00 4D AA
000048 00 68 2A 3A 00 00 20 BC 00 00 50 3C 00 68 4A F6 00 00
00005A 20 CB 00 00 4C C4 00 68 6B C1 00 00 20 83 00 00 4D BF
00006C 00 68 6C 44 00 00 20 23 00 00 4B 2A 00 68 AC 67 00 00
00007E 1F E1 00 00 48 D8 00 68 CC 48 00 00 20 84 00 00 4D 5A
000090 00 68 EC CC 00 00 21 1D 00 00 4E 12 00 69 OD E9 00 00
0000A2 21 42 00 00 50 24 00 69 2F 2B 00 00 24 0D 00 00 54 2D
0000B4 00 69 53 38 00 00 24 35 00 00 54 C1 00 69 77 6D 00 00
0000C6 23 84 00 00 50 E7 00 69 9A F1 00 00 28 24 00 00 7A 8E
0000D8 00 69 C3 15 00 00 22 CD 00 00 50 D6 00 69 E5 E2 00 00
0000EA 21 3E 00 00 52 CF 00 6A 07 20 00 00 1F F3 00 00 4B C0

Hmmm
Looks like
[ [ [ ] ]
[start addr]
[end addr]
[ UAT ]
[ payload ]
[ payload ]
[ .......... ]

BootSPIRom: reads image size and checksum

28C3/12.29.2011
Will not reveal checksum specifics, but...

I stared, I won.

If you stare, you probably will win too...
Security Analysis

```
. 0000002F  C  VerifyUSBID: NO MATCH, was %s, should be: %s\n
. 0000003D  C  VerifyUSBID: NO MATCH, USBID sent: %s, USBID should be: %s\n
. 0000004E  C  VerifyFWKey: NVRAM Key: 0x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x\n
. 0000004E  C  VerifyFWKey: Sent Key: 0x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x\n
. 0000003D  C  VerifyFWKey: NO MATCH at byte %d – NVRAM:0x%2x Sent:0x%2x \n
. 00000039  C  VerifyFWKey: Super Secret Bypass of Crypto-Key enabled\n
. 0000005B  C  VerifyPlatformID: ERROR: Invalid ID info version. Should be %d, %d, %d or %d, sent: %d.\n
. 0000002A  C  ACLBurnFlash: dataLen = %d, offset = %d\n
. 0000002C  C  ACLBurnFlash: Downloading %d bytes to %#x\n
. 0000002D  C  ACLBurnFlash: Boot bank %d, Target bank %d\n
. 00000039  C  ACLBurnFlash: FLASH sector size 0x%\x (\x boot sectors)\n```

HRM...

RFU CONTENT OBSERVATIONS:

• Specific version of compression library has known arb-code execution vulnerability.
RFU content observations:

- **Specific version of compression library has known arb-code execution vulnerability.**
- **No memory space separation**
- **No kernel-level security**
- **Everything runs as supervisor mode on CPU**
- **Any vulnerability in any (unprivileged) code will lead to full compromise**
RFU content observations:

• Specific version of compression library has known arb-code execution vulnerability.

• No memory space separation
• No kernel-level security
• Everything runs as supervisor mode on CPU
• Any vulnerability in any (unprivileged) code will lead to full compromise

• But there is no need because of the RFU Vulnerability…
POC TIME!

CRAFTING POC ATTACK

• WROTE RFU PACKER (200 LINES OF PYTHON)

I EVEN WROTE UNITTESTS!
Writing VxWorks Rootkit:

• ~3KB of ARM Assembly
• Print-Job Interceptor
• Reverse IP Proxy
• Debug-message Redirection (console to Telnet)
• Engine-Control Controller (cause paper jams, etc)
Poc time!

Crafting PoC Attack

- Wrote RFU Packer (200 lines of python)
  - Input: Arbitrary ELF Binary
  - Output: Single PJL Command
POC time!

Crafting PoC Attack

- **Wrote RFU Packer (200 lines of python)**
  - Input: Arbitrary ELF Binary
  - Output: Single PJL Command

- **Reworked Symbiote Tool-set**
  - Cross-compile Malware Code
  - Inject function hooks

- Input: Unpacked 2055DN VxWorks Image
  - Output: Malware-Injected VxWorks Image
POC time!

Writing VxWorks Rootkit:

Socketlib was a little tricky to find, but...
<table>
<thead>
<tr>
<th>Offset</th>
<th>Module</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000012</td>
<td>sockapi/trclosc.c</td>
<td>close</td>
<td>Socket close function</td>
</tr>
<tr>
<td>00000006</td>
<td>sockapi/trclosc.c</td>
<td>tfClose</td>
<td>Error message for socket close</td>
</tr>
<tr>
<td>00000008</td>
<td>sockapi/trclosc.c</td>
<td>socket has wrong ownership</td>
<td>Error message for socket ownership</td>
</tr>
<tr>
<td>00000018</td>
<td>sockapi/trclosc.c</td>
<td>Could not delete socket from tree</td>
<td>Error message for failed socket deletion</td>
</tr>
<tr>
<td>00000022</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000023</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000000</td>
<td>sockapi/trclosc.c</td>
<td>connect</td>
<td>Socket connect function</td>
</tr>
<tr>
<td>00000008</td>
<td>sockapi/trclosc.c</td>
<td>tflctl</td>
<td>Error message for tfctl</td>
</tr>
<tr>
<td>00000012</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000000</td>
<td>sockapi/trclosc.c</td>
<td>listen</td>
<td>Socket listen function</td>
</tr>
<tr>
<td>00000007</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000013</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000005</td>
<td>sockapi/trclosc.c</td>
<td>recv</td>
<td>Socket recv function</td>
</tr>
<tr>
<td>00000005</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000011</td>
<td>sockapi/trclosc.c</td>
<td>recvfrom</td>
<td>Error message for recvfrom</td>
</tr>
<tr>
<td>00000009</td>
<td>sockapi/trclosc.c</td>
<td>assertion error line %d, file(%s)</td>
<td>Error message for assertion error</td>
</tr>
<tr>
<td>00000023</td>
<td>sockapi/trclosc.c</td>
<td>sockapi/trsend.c</td>
<td>Error message for send function</td>
</tr>
</tbody>
</table>

**Title:** Print Me If You Dare

**Subtitle:** Firmware Update Attack and the Rise of Printer Malware
Mystery programmer, you are **awesome**!

**POC TIME!**

Lots of other juicy info in the unpacked image...
Technical Details: Malware-Injected RFU Build Process

- Cross-Compile hooks and Payload

Prereq: arm-elf tool chain python

`builds in os x`

PoC time!

```
dyn-209-2-218-2:rootkit ang$ cat Makefile
ARM_AS=/usr/local/arm/bin/arm-elf-as
CARVEBIN=../..src/CarveBin.py
SLICENDICE=../..src/SliceNDice.py

# Disassembly POC

---

clean:
  rm *.o

assemble:
  ${ARM_AS} -EB -k test.as -o test.o
  ${ARM_AS} -EB -k hook.as -o hook.o
  ${ARM_AS} -EB -k hook_paris.as -o hook_paris.o
  ${ARM_AS} -EB -k hook_snipsnip.as -o hook_snipsnip.o
  ${ARM_AS} -EB -k hook_snipsnip_syslog.as -o hook_snipsnip_syslog.o
  ${ARM_AS} -EB -k hook_snipsnip_icmp.as -o hook_snipsnip_icmp.o
  ${ARM_AS} -EB -k hook_snipsnip_icmp2.as -o hook_snipsnip_icmp2.o
  ${ARM_AS} -EB -k hook_snipsnip_ipv4.as -o hook_snipsnip_ipv4.o
  ${ARM_AS} -EB -k hook_printf.as -o hook_printf.o
  ${ARM_AS} -EB -k hook_icmp.as -o hook_icmp.o
  ${ARM_AS} -EB -k hook_printlog.as -o hook_printlog.o
  ${ARM_AS} -EB -k hook_printintercept.as -o hook_printintercept.o

  ${ARM_AS} -EB -k payload.as -o payload.o

arm-elf-ld -Ttext 0x15a670c -EB -s payload.o -o payload-linked.o
```
Poc Time!

Technical Details: Malware-Injected RFU Build Process

- Cross-Compile hooks and payload
- Inject binary into unpacked VxWorks Image

```python
python ${CARVEBIN} hook1.o
python ${CARVEBIN} print-linked.o
python ${CARVEBIN} printlog-linked.o

slicendice: carvebin
    python ${SLICENDICE} uncompressed-0-template uncompressed-0-instance

install: slicendice
    cp uncompressed-0-instance ./newfirmware/outbound/uncompressed-0

all: assemble carvebin slicendice install
```
POC TIME!

**Technical Details: Malware-Injected RFU Build Process**

- **Cross-Compile hooks and Payload**
- **Inject binary into unpacked VxWorks Image**
- **Run packer with altered VxWorks Image**

```
dyn-209-2-210-2:newfirmware ang$ cat Makefile
all:
  python packfirmware.py final-firmware-tramp
  lpr final-firmware-tramp.rfu
```

(AND PRINT TO PWN)
Poc time!

Technical Details: Malware-Injected RFU Build Process

- PoC code -> Inside a new RWX ELF Segment

```
addsect: ./arm/bin/arm-elf-objcopy -v --add-section .launchpad=newsection --change-section-address
```
Technical Details: Malware-Injected RFU Build Process

- PoC code -> Inside a new RWX ELF Segment

PoC time!

```
addsection:
./arm/bin/arm-elf-objcopy -v --add-section .launchpad=newsection --change-section-address
```

- Cross-compile with the right memory offset...

```
${ARM_AS} -EB -k control_tasktest.as -o control_tasktest.o
arm-elf-ld -Ttext 0x15CBFF0 -EB -s control_tasktest.o -o control_tasktest-linked.o
```
Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware

We sacrifice to the demo gods
PUTTING POC TOGETHER

OBVIOUS ATTACK VECTORS

• ACTIVE: Directly connect to 9100/TCP of target printer

• REFLEXIVE: Embed RFU in document, and use CUPS
Quantitative Scope

Active Attack:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

So who leaves their printers on the internet?
Quantitative Scope

Active Attack:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

So who leaves their printers on the internet?

75,000 Vulnerable Printers Online
Quantitative Scope

Fun stats gathered by our vulnerable embedded device scanner

- Total Vulnerable Printer Count: 76,995
Quantitative Scope

Fun stats gathered by our vulnerable embedded device scanner

- Total Vulnerable Printer Count: 76,995
- Government Printer Count: 43, 16 in the US
Quantitative Scope

Fun stats gathered by our vulnerable embedded device scanner

- **Total Vulnerable Printer Count**: 76,995
- **Government Printer Count**: 43, 16 in the US
- **Printers named “PAYROLL”**: 9, all EDU’s
Quantitative Scope

Active Attack:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

Does the active attack work on Windows?

I have a funny story in my backup slides…
Quantitative Scope

Reflexive Attack:

HP also highlighted the fact that all of its printers from 2009 onwards include digital signing to prevent this type of exploit, but the researchers said that still leaves tens of millions of devices vulnerable.

The security flaw on the pre-2009 machines allows hackers to send customised firmware to a printer that could enable them to render a user's printer useless, waste toner or overheat the device.

Wrong! 2009 doesn’t mean what you think it means (and apparently HP never said 2009)

Quantitative Scope

Reflexive Attack:

HP also highlighted the fact that all of its printers from 2009 onwards include digital signing to prevent this type of exploit, but the researchers said that still leaves tens of millions of devices vulnerable.

The security flaw on the pre-2009 machines allows hackers to send customised firmware to a printer that could enable them to render a user’s printer useless, waste toner or overheat the device.

How many LaserJet units did HP ship in 2005-NOW?

REFLEXIVE ATTACK:

HP also highlighted the fact that all of its printers from 2009 onwards include digital signing to prevent this type of exploit, but the researchers said that still leaves tens of millions of devices vulnerable.

The security flaw on the pre-2009 machines allows hackers to send customised firmware to a printer that could enable them to render a user's printer useless, waste toner or overheat the device.

How many LaserJet units did HP ship in 2005-NOW?

Have you used one this year? (probably)
Reflexive PS Attack

Print Me If You Dare

Firmware Update Attack and the Rise of Printer Malware

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

28C3/12.29.2011
REFLEXIVE PS ATTACK

Columbia University
In the City of New York
This applies to HP P2030/P2050 models

- (many) other models vulnerable
- At least 3 other (unsigned) RFU formats

- Printers running LynxOS, VxWorks, etc have slightly different RFU formats

- Attack Vectors the same
- RFU formats are slightly different
  - Just repeat the same exercise!
# Print Me If You Dare

**Firmware Update Attack and the Rise of Printer Malware**

<table>
<thead>
<tr>
<th>Printer Model</th>
<th>ISA</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>2055</td>
<td>ARM</td>
<td>VxWorks</td>
</tr>
<tr>
<td>2030</td>
<td>ARM</td>
<td>VxWorks</td>
</tr>
<tr>
<td>2410</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>24x0</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>3000</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>3800</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4005</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4100</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4240</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Printer Model</th>
<th>ISA</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>5025</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>5035</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>3505</td>
<td>PowerPC!</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4250</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4345</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4350</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4600</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4650</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4700</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>4730</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>5200</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>5500</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>5550</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>6015</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
<tr>
<td>9050</td>
<td>MIPS</td>
<td>LynxOS</td>
</tr>
</tbody>
</table>

Quick unpack, grep for “LynxOS” in the ELF image
Double check yourself!

---

Thanks Jon Voris!
You can verify vulnerability of your printers easily!

1. **Lockdown your printer according to HP NIST GUIDE**
2. **Download RFU from HP**
3. **LPR the RFU, see if it works…**

General Mitigation (Immediate)

- Disable RFU Updates (possible, but not on all models)
GENERAL MITIGATION (IMMEDIATE)

- Disable RFU Updates (possible, but not on all models)
- Apply ACL, passwords (use Web JetAdmin)
- Filter print-job content on print-server
- Isolate printers from sensitive networks
General Mitigation (Immediate)

- Disable RFU Updates (possible, but not on all models)
- Apply ACL, passwords (use Web JetAdmin)
- Filter print-job content on print-server
- Isolate printers from sensitive networks

- But on the 2055DN...

- RFU Update could not be disabled using WJA
- PJL password did not prevent “PJL ENTER LANGUAGE=ACL”
- Cannot prevent RFU attack!
- HP is working on a fix for printers like this...
General Mitigation (Immediate)

- Disable RFU Updates (possible, but not on all models)
- Apply ACL, passwords (use Web JetAdmin)
- Filter print-job content on print-server
- Isolate printers from sensitive networks

Do this quickly. It’s a race!

First thing I’d do (If I’m the bad guy):

- Disable further RFU updates
- Inject Malware into SPI-Flash
- Lock all FLASH pages
# Print Me If You Dare

**Firmware Update Attack and the Rise of Printer Malware**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>One Byte Command Code</th>
<th>Description</th>
<th>Address Bytes</th>
<th>Mode Bit Cycle</th>
<th>Dummy Bytes</th>
<th>Data Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ</td>
<td>(03h)</td>
<td>0000 0011</td>
<td>Read Data bytes</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>FAST_READ</td>
<td>(0Bh)</td>
<td>0000 1011</td>
<td>Read Data bytes at Fast Speed</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>DOR</td>
<td>(3Bh)</td>
<td>0011 1011</td>
<td>Dual Output Read</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>QOR</td>
<td>(6Bh)</td>
<td>0110 1011</td>
<td>Quad Output Read</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>DIOR</td>
<td>(BBh)</td>
<td>1011 1011</td>
<td>Dual I/O High Performance Read</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>QIOR</td>
<td>(EBh)</td>
<td>1110 1011</td>
<td>Quad I/O High Performance Read</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>RIDID</td>
<td>(9Fh)</td>
<td>1001 1111</td>
<td>Read Identification</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>READ_ID</td>
<td>(90h)</td>
<td>1001 0000</td>
<td>Read Manufacturer and Device Identification</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td><strong>Write Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WREN</td>
<td>(06h)</td>
<td>0000 0010</td>
<td>Write Enable</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WRDI</td>
<td>(04h)</td>
<td>0000 0100</td>
<td>Write Disable</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Erase</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P4E</td>
<td>(20h)</td>
<td>0010 0000</td>
<td>4 KB Parameter Sector Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>P8E</td>
<td>(40h)</td>
<td>0100 0000</td>
<td>8 KB (two 4 KB) Parameter Sector Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SE</td>
<td>(D8h)</td>
<td>1101 1000</td>
<td>64 KB Sector Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BE</td>
<td>(60h)</td>
<td>0110 0000 or (C7h)</td>
<td>Bulk Erase</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Program</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PP</td>
<td>(02h)</td>
<td>0000 0010</td>
<td>Page Programming</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to 256</td>
</tr>
<tr>
<td>QPP</td>
<td>(32h)</td>
<td>0111 0010</td>
<td>Quad Page Programming</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to 256</td>
</tr>
<tr>
<td><strong>Status &amp; Configuration Register</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDSR</td>
<td>(09h)</td>
<td>0000 0101</td>
<td>Read Status Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>WRR</td>
<td>(01h)</td>
<td>0000 0001</td>
<td>Write (Status &amp; Configuration) Registers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to 2</td>
</tr>
<tr>
<td>RCR</td>
<td>(35h)</td>
<td>0011 0101</td>
<td>Read Configuration Register (CFG)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
<tr>
<td>CLSR</td>
<td>(30h)</td>
<td>0011 0000</td>
<td>Reset the Erase and Program Fail Flag (SR5 and SR6) and restore normal operation</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td><strong>Power Saving</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP</td>
<td>(B0h)</td>
<td>1011 1001</td>
<td>Deep Power-Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RES</td>
<td>(ABh)</td>
<td>1010 1011</td>
<td>Release from Deep Power-Down Mode</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>OTP</td>
<td>(42h)</td>
<td>0100 0010</td>
<td>Programs one byte of data in OTP memory space</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>OTPR</td>
<td>(4Bh)</td>
<td>0100 1011</td>
<td>Read data in the OTP memory space</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1 to ∞</td>
</tr>
</tbody>
</table>
EMBEDDED
DEFENSE
THE
BIGGER
PICTURE
Digitally Signed Firmware
Digitally Signed Firmware

==

Secure Firmware?
What if Microsoft said…

Windows is secure because we only allow code signed by Microsoft. That means you can’t run your own anti-virus code, but don’t worry…. It’s all good!

You would probably say…
What if HP said…

LaserJet is secure because we only allow code signed by HP. That means you can’t run your own anti-virus code, but don’t worry… It’s all good!

You would probably say…
REAL EMBEDDED DEFENSE!
Real Defense!

- Host-based Embedded Defense NEEDS to EXIST
Real Defense!

- **Host-based Embedded Defense** NEEDS to exist
- **Defense should be** well-known
- **No more obscure secret-sauce security**
Real Defense!

- Host-based Embedded Defense NEEDS to exist
- Defense should be well-known
- No more obscure secret-sauce security
- Defense should be decoupled from OS
Real Defense!

- **Host-based Embedded Defense NEEDS to exist**
- Defense should be well-known
- No more obscure secret-sauce security
- Defense should be decoupled from OS
- OS fortification is good
  - But should not replace **Independent Security Software**!
Real Embedded Defense Exists today!

Tested on Cisco IOS

- Cui, Stolfo RAID 2011
- Cui, Kataria, Stolfo ACSAC 2011
- Cui, Kataria, Stolfo Blackhat 2011
Real Embedded Defense Exists today!

Tested on Cisco IOS
- Cui, Stolfo RAID 2011
- Cui, Kataria, Stolfo ACSAC 2011
- Cui, Kataria, Stolfo Blackhat 2011

Want a router sensor? Email me!

Print Me If You Dare
Firmware Update Attack and the Rise of Printer Malware
Real Embedded Defense Exists today!

Tested on Cisco IOS

- Cui, Stolfo RAID 2011
- Cui, Kataria, Stolfo ACSAC 2011
- Cui, Kataria, Stolfo Blackhat 2011

Applied HP (hopefully)

- Coming In 2012!
23. Are current HP multifunction printers susceptible to viruses and worms?
No, since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. HP MFPs use non-standard operating systems other than Windows. Consequently, they are immune to these viruses and worms. In practice, there have been no known instances of viruses or worms infecting HP MFPs.

In the future HP will likely ship MFPs which include an embedded version of the Windows operating system. However, there are a number of practical reasons why this won't increase the security risk faced by customers.

24. Does this mean that HP MFPs are completely safe from worms and viruses?
No, since it is technically possible for someone to craft a virus or worm that targets the non-standard operating systems shipped with the MFPs. However, HP considers the probability of such an event to be considerably lower. Hackers are more likely to be interested in exploiting vulnerabilities in workstations and servers since they are more widespread and require less expertise.

Questions!

IN LOVING MEMORY OF
BAM BAM
ENGINE CONTROLLER: NEC Microcontroller on All Models I looked at.

NEC
RH4-0296-02
RH4-5410-01
RH4-0214-05
RK2-0922-02
RK2-2718-02

Programmable Via RFU!
ENGINE CONTROLLER:

**NEC** Microcontroller on All Models I looked at.

Great place for malware to hide...
Search for “HP Columbia Printer”

Please don’t attack us.

We surrender!

-(}
Offensive Potential

We intentionally did not “weaponize” this attack

But can this be done practically on Windows?
Offensive Potential

Speaking of MS Word...

Field codes: Print field
Applies to: Microsoft Office Word 2003

{ PRINT "PrinterInstructions" }

Sends printer-control code characters to the selected printer. Microsoft Word displays a result only when the document is printed. For appropriate printer codes, consult your printer manual.

+ Learn more about using the PRINT field to embed PostScript commands in a document

NOTE The PRINT field works well with a PostScript printer or a Hewlett-Packard LaserJet printer, but it may not work properly with another type of laser printer. The PRINT field works with a dot-matrix printer only if the printer supports the PassThrough command.

Did this article help you?

Yes  No  Not what I was looking for
Field codes: Print field
Applies to: Microsoft Office Word 2003

{ PRINT "PrinterInstructions" }

Sends printer-control code characters to the selected printer. Microsoft Word displays a result only when the document is printed. For appropriate printer codes, consult your printer manual.

Learn more about using the PRINT field to embed PostScript commands in a document

NOTE The PRINT field works well with a PostScript printer or a Hewlett-Packard LaserJet printer, but it may not work properly with another type of laser printer. The PRINT field works with a dot-matrix printer only if the printer supports the PassThrough command.

Did this article help you?

[Yes] [No] [Not what I was looking for]
Offensive Potential

Speaking of MS Word... (Funny story)

When low on man-power, outsource!
Hi Ang and Hemin,

My name is Albert Mah, a Support Escalation Engineer on the Word team. You were previously working with Ross Lindgren, who assigned your case to me and I will now be your main point of contact.

11101383378206 WD2007: Problem with Hexadecimal in .PRN file

As I understand it, you want to include approximately 7MB of raw PJL data in a Print field and sent it to a printer. However, your finding that the hex sequence

a) "BF FA FE 00 00 00" is being inserted into the .prn file when using an HP PCL6 driver

b) “1B 2A 6F 34 57 0A 06 00 01 1B 2A 6F 34 57 0A 06 00 00” is being inserted into the .prn file when using an HP PCL5 or PS driver.

At this point, I’m investigating whether this sequence is being inserted by Word or not.

I’ll keep you posted on any new developments.

Have a great Halloween weekend!

Thank you for using Microsoft Customer Service and Support (CSS),

Albert Mah
Support Escalation Engineer | Commercial Technical Support

Office: (469) 775-6465
Fax: (555) 775-6738
Bridge (866) 500-6738 Passcode: 9866716
almah@Microsoft.com
microsoft.com/
Offensive Potential

Speaking of MS Word... (Funny story)

We can talk about it now because...
2. HP also released its latest Universal Print Driver (UPD) PCL6 (version 5.4) driver on December 1\textsuperscript{st}.
We installed the driver, and when we attempted to print the sample document to .prn file, we get the error:

This error can appear if a default printer has not been designated or if the application is unable to locate an existing default printer. To correct this problem, try one of the following in Microsoft Windows:

- If a printer or printer settings is not available after you click the \textbf{File} tab, and then click \textbf{Print}, add a printer.
- If the application cannot find an existing printer that is already installed, set the printer as the default printer.
- If a default printer is installed but the application is unable to use it, uninstall the printer driver, and then install the latest version of the printer driver.
- If the printer is on a print server, make sure the printer is available, the network is functioning, the server is not stalled, the printer is not out of paper, or the printer is not suspended by the administrator. Printing issues associated with a network printer are best handled by your local network administrator.

For more information about setting up and troubleshooting printer connections, see Windows Help and Support.
How it all started...

Applying Software Symbiote Defense to Printers

Applied to Cisco IOS

- Cui, Stolfo RAID 2011
- Cui, Kataria, Stolfo ACSAC 2011
- Cui, Kataria, Stolfo Blackhat 2011
How it all started...

Applying Software Symbiote Defense to Printers

Applied to Cisco IOS

- Cui, Stolfo RAID 2011
- Cui, Kataria, Stolfo ACSAC 2011
- Cui, Kataria, Stolfo Blackhat 2011

But can it be done to not-a-router?
For the Symbiote to work, you need to:
For the Symbiote to work, you need to:

- Unpack Existing Firmware
For the Symbiote to work, you need to:

- Unpack Existing Firmware
- Analyze Unpacked Binary
For the Symbiote to work, you need to:

- Unpack Existing Firmware
- Analyze Unpacked Binary
- Inject Symbiote Manager and Payload
FOR THE SYMBIOTE TO WORK, YOU NEED TO:

- **UNPACK EXISTING FIRMWARE**
- **ANALYZE UNPACKED BINARY**
- **INJECT SYMBIOTE MANAGER AND PAYLOAD**
- **REPACK FIRMWARE**
Quantitative Scope

Active Attack:

While HP has identified a potential security vulnerability with some HP LaserJet printers, no customer has reported unauthorized access. The specific vulnerability exists for some HP LaserJet devices if placed on a public internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade.

Who exactly is a “trusted party” on your network?
For the Symbiote to work, you need to:

- **Unpack Existing Firmware**
- **Analyze Unpacked Binary**
- **Inject Symbiote Manager and Payload**
- **Repack Firmware**

But first, you have to be able to modify the firmware on the target device...