Corporate Espionage

FOR

DUMMIES

The Hidden Threat of Embedded Web Servers

Michael Sutton
VP, Security Research

© 2009-2011 Zscaler, Inc.
Company

- Browser/email security
- VP, Security Research

Background

- Founding Member – Cloud Security Alliance
- SPI Dynamics – acquired by HP
- iDefense – acquired by VeriSign

Research

- Web security
- Client-side vulnerabilities
Agenda

1. Current State
2. Threats
3. Solutions
What does it mean to be in a hyperconnected world?
What has an IP address in your home?

- Television
- DVR
- Blu-ray/DVD
- Webcam
- Large Appliances
- Video Game Console
- Kitchen Appliances
- Phone
What has an IP address in your office?

- Printer
- Scanner
- Networking
- Security System
- HVAC
- NAS
- Video Conferencing
- Photocopier
What is an Embedded Web Server? There’s no universally accepted definition, but for our purposes, we’ll require the following:

1. Web server installed on the hardware during the manufacturing process (not an optional component)
2. Not designed for high performance
3. Limited functionality
4. Serves as an administrative interface to the host hardware
Attention!

No embedded web servers were harmed during the course of this research.

All examples come from publicly accessible web servers without password protection.
Threats

Overall

- DoS – Disable functionality
- Privacy – Access confidential data
- Data Integrity – Alter confidential data
- Financial – Unauthorized use of bandwidth and services
- Compromise – Firmware upgraded with new functionality

External

- Improperly configured networks can make internal appliances Internet accessible
- Vendors target *ease of use* and EWSs therefore have functionality enabled *out of the box* with a default password or are wide open

Internal

- Devices with EWS generally not considered during security audits and are not therefore monitored/segregated
- Insiders have the advantage of physical access to the devices
Java Vulnerabilities?

**Attacks?**

1. Change the preset coffee settings (make weak or strong coffee)
2. Change the amount of water per cup (say 300ml for a short black) and make a puddle
3. Break it by engineering settings that are not compatible (and making it require a service)

**Internet-connected coffee maker has security holes**

by Elmar Mills

An Australian man has discovered security vulnerabilities in his Internet-connected coffee maker that could allow a remote attacker to not only take over his Windows XP-based PC but also make his coffee too weak.

Craig Wright, a risk advisory services manager at professional services firm BDO, found several security holes, including a buffer overflow in the Internet Connection software that links his Jura F90 coffee maker to his PC.

Once connected to the Internet, the high-end coffee maker, which retails for nearly US$2,000 on Amazon, lets you do things like set the strength of your coffee and get remote diagnostic help over the Internet without having to send the appliance in for service.

Wright posted the information on the vulnerabilities, and the fact that there is no patch available yet, to the Bugtraq security e-mail list on Tuesday.

A U.S.-based public relations representative for the coffee maker said she would try to reach spokespersons in the Switzerland headquarters for comment.

The threat hasn't kept Wright awake at night, although the coffee does, he said in an interview with CNET News.com at 2:30 Wednesday morning Sydney time.

"I don't know if many people would target this particular vulnerability because there probably are not a lot of coffee makers at the moment that are Internet-connected, and in my case it's behind a firewall," he said.

However, Internet-connected appliances are the wave of the future. There is already an Internet-connected refrigerator, at least one prototype of a Web-enabled oven, and pilot tests for dryers and water heaters. (Credit: Jura)
Energy Savings

Internet-Connected Appliances Could Lower Energy Bills

A pilot test in Washington and Oregon lets dryers and water heaters check electricity prices and decide if it’s worth waiting until off-peak times.

By Keyla Kirton InformationWeek
May 15, 2006 12:00 AM

Jerry Brous’ clothes dryer drives a hard bargain. Every five minutes, it checks the current electricity price over the Internet. If the price is above the threshold Brous set, the dryer doesn’t run. Save the clothes for later—and don’t get soaked.

Brous is one of 200 people in Washington and Oregon taking part in an experiment that uses real-time pricing data to let people make smarter choices about energy use. It’s a tiny project with the potential to significantly change electricity markets at a time when energy is back on top of public policy concerns.

More Insights

White Papers
- How to Effectively Measure and Monitor Activity in Your Portal Environment
- Going Into School Teaching After Academic Study

Videos
Sponsored by:

- Energy savings and home automation will continue to drive Internet enabled devices
- Currently serves as a differentiator for high end appliances
- Combination of EWSs, HTTP(S) aware client side applications

Dryers and Water Heaters
The GridWise Initiative, led by the Pacific Northwest National Laboratory, is testing dryers, thermostats, and water heaters that are wirelessly connected to a server, which uses a broadband connection to fetch prices. Homeowners also can set monthly energy budgets and monitor in real time whether they’re sticking to them. In another experiment, 150 dryers are equipped with a chip that will respond to instability on the power grid and shut off the heating units on the dryers for a few minutes. Spread across millions of homes, this program could provide a shock absorber in the grid, giving producers the few minutes needed at times of peak demand to bring new power online.

The project takes a market approach to trying to lower power consumption—or shift it to off-peak times. That could let utilities put off building new power plants, says Don Hammerstrom, Pacific Northwest National Lab’s project manager.
Strange Sightings - Projectors

KEC-1003PJB
HP Digital Projector xp8020

Device Info

Status: Standby
Current lamp hours: 1242
System Contact: Albert Berglund
Support Phone Number: 541.737.6428
System Location: Kelley Engineering Center 1003

Firmware Version: 5.0 - 2.1
Wired IP Address: 128.193.38.152
Wireless IP Address: [Unknown]
Serial Number: *******
Admin Password: [Set]

HTTP/1.1 200 OK
Server: microChai ver 2.0
Cache-Control: no-cache
Expires: Mon, 24 Nov 2003 00:00:00 GMT
Connection: Keep-Alive
Transfer-Encoding: chunked
Strange Sightings - Projectors

Tip!

Office Prank
Step 1 – Scan the network for web servers with the following header:
  Server: Network Projector
Step 2 – Wait for the meeting to start
Step 3 – Continually adjust focus. When presenter attempts to fix, power off.
Strange Sightings - Printers

If you’re too lazy to walk over to the printer to check the ink cartridges...

...you’re also too lazy to walk to the store to replace them!

© 2009-2011 Zcaler, Inc.
Strange Sightings - Kiosks

Welcome!
Are you ready to search over a million pairs of shoes?
How would you like to search?
- Brand
- Size
- Different size or color
- Style

Please swipe your Badge

UCLA General Services

© 2011 UCLA General Services. All Rights Reserved.
**Goal**

- Fingerprint at least 1M web servers and identify as many EWSs as possible to better understand the threat that they may pose

**Challenges**

- Millions of IP addresses need to be scanned
- Scanning must therefore be very light weight and scalable
- Existing fingerprinting tools (i.e. NMAP) do not have a strong database of EWS data

**Options**

- Traditional scanning/fingerprinting tools
- GHDB (Google Hacking Database)
- Header fingerprinting scans
Nmap Results
$ sudo nmap -O 131.96.246.162
[snip]
Aggressive OS guesses: Apple AirPort Express WAP v6.3 (92%), AirSpan ProST WiMAX access point (91%), m0n0wall FreeBSD-based embedded firewall version 1.22 - 1.23b1 (89%), Canon imageRUNNER C5185 printer (89%), SonicWALL SonicOS Enhanced 5.2.0.1-21o (88%), FreeBSD 6.2-RELEASE (88%), VxWorks: Apple AirPort Extreme v5.7 or AirPort Express v6.3; Canon imageRUNNER printer (5055, C3045, C3380, or C5185); Kyocera FS-4020DN printer; or Xerox Phaser 8860MFP printer (87%), IBM DCS9900 NAS device (87%), Nokia IP650 firewall (IPSO 4.0 and CheckPoint Firewall-1/VPN-1 software) (85%), HP LaserJet P2055dn printer (85%) No exact OS matches for host (test conditions non-ideal).

Server Headers
HTTP/1.1 200 OK
Date: SUN, 16 JUL 2011 19:13:57 GMT
Server: CANON HTTP Server Ver2.21
Content-Type: text/html
Transfer-Encoding: chunked
GHDB

Remote UI

Device Name: iR2270
Product Name: iR2270
Location: NW011

Printer Status: Ready to print.
Scanner Status: Ready to scan.

System Manager: RadIS Support
Support:

Last Updated: 05/16/2011 13:15:33

Language: English
リモートUI
Copyright CANON INC. 2006
All Rights Reserved

製品名： iR C2570

最終更新：2011年05月17日 05:15:00

プリンタ：スリープ中です。
スキャナ：スリープ中です。
ファックス：ファックスできます。

表示言語の切替： Japanese

システム管理者：
サポートリンク：
Challenges

- Google clearly suppresses/blocks GHDB queries (Bing can actually be better)
- UI Internationalization/rebranding requires many queries for broad coverage
- API queries are throttled to a set amount per day
- Searches for potentially vulnerable systems can lead to source IP blocks, especially when queries are automated
Header Scanning

HTTP/1.0 200 OK
Date: SUN, 23 APR 2011 21:31:45 GMT
Server: CANON HTTP Server Ver2.21
Set-Cookie: iR=3753281; path=/
Content-Type: text/html
Transfer-Encoding: chunked

Approach
• Simple multi threaded Perl script to send HEAD requests
• Amazon EC2 micro instances leveraged – highly scalable, low cost

Advantages
• Highly scalable – small request/response
• Ease of automation
• Content based signatures not required
• EWS header information unlikely to be spoofed

Limitations
• Not all EWSs have a unique Server string or header info.

Result
• Goal of fingerprinting 1M web servers achieved
Shodan

- Comprehensive, searchable database of web server headers and telnet banners
- Provides country of origin IP and rDNS data
- Commercial service – users must register to receive >10 results and pay for >50
Agenda

2 Threats

What could possibly go wrong?
Printers/Scanners

“Mistakes are the portals of discovery”
- James Joyce (1882-1941)
## HP Printers/Scanners

### Table of Embedded Web Servers

<table>
<thead>
<tr>
<th>Headers</th>
<th>LaserJet</th>
<th>OfficeJet</th>
<th>Photosmart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: Mrvl-R1_0</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: $ProjectRevision: 5.0.1.23 $</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: $ProjectRevision: 4.2 $</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: $ProjectRevision: 4.0.2.38 $</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Server: $ProjectRevision: 4.7.1.12 $</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Server: HP-ChaiServer/3.0</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SERVER: HP-ChaiSOE/1.0</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Server: Virata-EmWeb/R6_2_1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Numerous embedded web servers across hundreds of products
## HP Printers/Scanners

### Headers

<table>
<thead>
<tr>
<th>Headers</th>
<th>ShodanHQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: Mrvl-R1_0</td>
<td>22</td>
</tr>
<tr>
<td>Server: $ProjectRevision: 5.0.1.23 $</td>
<td>673</td>
</tr>
<tr>
<td>Server: $ProjectRevision: 4.2 $</td>
<td>1,498</td>
</tr>
<tr>
<td>Server: $ProjectRevision: 4.0.2.38 $</td>
<td>4,514</td>
</tr>
<tr>
<td>Server: $ProjectRevision: 4.7.1.12 $</td>
<td>946</td>
</tr>
<tr>
<td>Server: HP-ChaiServer/3.0</td>
<td>18,011</td>
</tr>
<tr>
<td>SERVER: HP-ChaiSOE/1.0</td>
<td>39,071</td>
</tr>
<tr>
<td>Server: Virata-EmWeb/R6_2_1</td>
<td>59,269</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>124,004</strong></td>
</tr>
</tbody>
</table>

### Admin Password Set for Identified Scanners?

<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Photocart</td>
<td>36%</td>
<td>64%</td>
</tr>
</tbody>
</table>

*Note: The chart shows the percentage of identified scanners with and without admin passwords set.*
### Purpose

- Manage devices – security, logging, networking, etc.
- Monitor devices – ink levels, alerts, etc.

### Observations

- Laserjet printers rarely have password protection enabled
- Hundreds of thousands of HP devices are web accessible

### Risk

- Reconfigure device – networking, UI, etc.
- DoS – lock device access, cancel jobs, etc.
- WebScan – remotely access scans and trigger new jobs
- Fax Forwarding – forward incoming faxes
Forward all incoming faxes to an external fax number.
HP Webscan

Quick Scan – Determine if doc. exists
Scan and download as JPEG
What we found...

Signed documents
What we found...

<table>
<thead>
<tr>
<th>Name</th>
<th>Party</th>
<th>Vote</th>
</tr>
</thead>
<tbody>
<tr>
<td>BILL CHAMBERS</td>
<td>Republican</td>
<td>7</td>
</tr>
<tr>
<td>KEN MILLER</td>
<td>Republican</td>
<td>8</td>
</tr>
<tr>
<td>DOUGLAS B. HUGHES</td>
<td>Republican</td>
<td>9</td>
</tr>
<tr>
<td>LAWRENCE &quot;LARRY&quot; NARITELI</td>
<td>Republican</td>
<td>10</td>
</tr>
<tr>
<td>ROBERT G. NEWMAN B</td>
<td>Republican</td>
<td>11</td>
</tr>
<tr>
<td>DAVID RULLY SMITH</td>
<td>Republican</td>
<td>12</td>
</tr>
<tr>
<td>MW WHITMAN</td>
<td>Republican</td>
<td>13</td>
</tr>
<tr>
<td>STEVE POZNER</td>
<td>Republican</td>
<td>14</td>
</tr>
<tr>
<td>SAM AAKSTAD</td>
<td>Republican</td>
<td>15</td>
</tr>
<tr>
<td>YVONNE H. GIARD</td>
<td>Republican</td>
<td>16</td>
</tr>
<tr>
<td>BERN DAVIS</td>
<td>Republican</td>
<td>17</td>
</tr>
<tr>
<td>ABEL VALDANO</td>
<td>Republican</td>
<td>18</td>
</tr>
<tr>
<td>DAVE HARRIS</td>
<td>Republican</td>
<td>19</td>
</tr>
<tr>
<td>SCOTT L. LEVITT</td>
<td>Republican</td>
<td>20</td>
</tr>
<tr>
<td>DAMON DUNN</td>
<td>Republican</td>
<td>21</td>
</tr>
<tr>
<td>ORLY TATZ</td>
<td>Republican</td>
<td>22</td>
</tr>
<tr>
<td>SAM EVANS</td>
<td>Republican</td>
<td>23</td>
</tr>
<tr>
<td>TONY STRICKLAND</td>
<td>Republican</td>
<td>24</td>
</tr>
<tr>
<td>MIAMI WALLACE</td>
<td>Republican</td>
<td>25</td>
</tr>
</tbody>
</table>

Voting advice
HP Webscan

What we found...

Signed checks
HP Webscan

What we found...

Technical reports
HP Webscan

What we found...

Forms
Jim is a Certified Mold Inspector!
HP Webscan

**Prevalence**
- HP scanners for several years have included Webscan functionality

**Risk**
- Webscan functionality enabled by default without password protection
- Many networks are misconfigured to expose scanners

**Automation**
- `http://[Scanner IP]/scan/image1.jpg?id=1&type=4&size=1&fmt=1&time=[epoch time]`
- Predictable URL path for scanned documents
- Request above URL every second to retrieve any scanned documents
Photocopiers

“Copy from one, it's plagiarism; copy from two, it's research.”

- Wilson Mizner (1876 - 1933)
# Xerox Photocopiers

<table>
<thead>
<tr>
<th>Shodan Results</th>
<th>Shodan Results</th>
<th>Shodan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Query → “Spyglass_MicroServer/2.01FC1”</td>
<td>• Query → “Spyglass_MicroServer/2.00FC4”</td>
<td>• Query → “Xerox_MicroServer/Xerox11”</td>
</tr>
<tr>
<td>• Results → 427</td>
<td>• Results → 32</td>
<td>• Results → 724</td>
</tr>
<tr>
<td>• Server string alone offers unique identifier</td>
<td>• Tektronix copiers (Phaser branded copiers sold to Xerox in 1999)</td>
<td>• Xerox Workcentre</td>
</tr>
</tbody>
</table>
## Job Accounting

- **File name**
- **User name**
- **Pages**
- **Date**
- **Time**

### Xerox Photocopiers

**CentreWare Internet Services**

**Phaser 6200**

This page displays the 10 oldest job accounting records. Use the links at the bottom of the page to view other records. Use the small type version for easier printing.

<table>
<thead>
<tr>
<th>Job Index</th>
<th>Protocol</th>
<th>User Name</th>
<th>Host Name</th>
<th>File Name</th>
<th>Job Name</th>
<th>Pages/Sheets Printed</th>
<th>Pages/Sides Printed</th>
<th>Start Time</th>
<th>End Time</th>
<th>Interpreter Duration</th>
<th>Paper Type</th>
<th>Paper size</th>
<th>Cyan Used</th>
<th>Magenta Used</th>
<th>Yellow Used</th>
<th>Black Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>BCE ABET Outcomes &amp; Performance Criteria 2011 - 07.27.xls</td>
<td>BCE ABET Outcomes &amp; Performance Criteria 2011 - 07.27.xls</td>
<td>3</td>
<td>3</td>
<td>7/20/2011 12:28:21</td>
<td>7/20/2011 12:28:23</td>
<td>0:00:03</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0051%</td>
<td>0.0399%</td>
<td>0.0693%</td>
<td>0.0569%</td>
</tr>
<tr>
<td>2</td>
<td>IPP</td>
<td>Joe</td>
<td>157.229.71.157</td>
<td>IPP_Job</td>
<td>IPP_Job</td>
<td>3</td>
<td>3</td>
<td>7/20/2011 14:13:16</td>
<td>7/20/2011 14:13:22</td>
<td>0:00:04</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0031%</td>
<td>0.0000%</td>
<td>0.0000%</td>
<td>0.0377%</td>
</tr>
<tr>
<td>3</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>ECE Course Instructor Schedule 2011.doc</td>
<td>ECE Course Instructor Schedule 2011.doc</td>
<td>1</td>
<td>1</td>
<td>7/23/2011 15:15:55</td>
<td>7/23/2011 15:15:56</td>
<td>0:00:01</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0002%</td>
<td>0.0000%</td>
<td>0.0012%</td>
<td>0.0126%</td>
</tr>
<tr>
<td>4</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>ECE Course Instructor Schedule 2011.doc</td>
<td>ECE Course Instructor Schedule 2011.doc</td>
<td>1</td>
<td>1</td>
<td>7/23/2011 15:17:15</td>
<td>7/23/2011 15:17:16</td>
<td>0:00:01</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0002%</td>
<td>0.0000%</td>
<td>0.0012%</td>
<td>0.0126%</td>
</tr>
<tr>
<td>5</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>ECE Course Instructor Schedule 2011.doc</td>
<td>ECE Course Instructor Schedule 2011.doc</td>
<td>1</td>
<td>1</td>
<td>7/23/2011 15:17:25</td>
<td>7/23/2011 15:17:26</td>
<td>0:00:01</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0002%</td>
<td>0.0000%</td>
<td>0.0012%</td>
<td>0.0126%</td>
</tr>
<tr>
<td>6</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>BCE ABET Outcomes &amp; Performance Criteria 2011 - 07.27.xls</td>
<td>BCE ABET Outcomes &amp; Performance Criteria 2011 - 07.27.xls</td>
<td>1</td>
<td>1</td>
<td>7/23/2011 15:21:17</td>
<td>7/23/2011 15:21:20</td>
<td>0:00:03</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0100%</td>
<td>0.0100%</td>
<td>0.0231%</td>
<td>0.0329%</td>
</tr>
<tr>
<td>7</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>Microsoft Word - Monastic Speaker Schedule 2011.doc</td>
<td>Microsoft Word - Monastic Speaker Schedule 2011.doc</td>
<td>3</td>
<td>3</td>
<td>7/30/2011 14:20:58</td>
<td>7/30/2011 14:20:59</td>
<td>0:00:04</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0002%</td>
<td>0.0008%</td>
<td>0.0000%</td>
<td>0.0185%</td>
</tr>
<tr>
<td>8</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>Microsoft Word - Monastic Speaker Schedule 2011.doc</td>
<td>Microsoft Word - Monastic Speaker Schedule 2011.doc</td>
<td>4</td>
<td>4</td>
<td>7/30/2011 14:27:26</td>
<td>7/30/2011 14:27:26</td>
<td>0:00:03</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0003%</td>
<td>0.0011%</td>
<td>0.0000%</td>
<td>0.0251%</td>
</tr>
<tr>
<td>9</td>
<td>AppSocket</td>
<td>Charlie</td>
<td>157.229.71.126</td>
<td>DegreeWorks by SunGold Higher Education DegreeWorks 4.07 DOGWP UAF</td>
<td>DegreeWorks by SunGold Higher Education DegreeWorks 4.07 DOGWP UAF</td>
<td>1</td>
<td>1</td>
<td>7/30/2011 16:45:38</td>
<td>7/30/2011 16:45:38</td>
<td>0:00:02</td>
<td>Plain Paper</td>
<td>Letter</td>
<td>0.0003%</td>
<td>0.0002%</td>
<td>0.0001%</td>
<td>0.0012%</td>
</tr>
</tbody>
</table>
Need a place to store your warez?

- FTP server enabled by default
- No password
Xerox Photocopiers

Web Links

The Web Links page contains special links to Xerox internet sites so that you can easily access printer documentation, software, service and supplies. Alternatively, you can enter custom URLs in the fields below to access your own network files or internet for desired content.

In the fields below, select "Xerox link" to continue using the default links, or select "Custom link" and enter your custom URL.

Software Links

<table>
<thead>
<tr>
<th>Printer Drivers</th>
<th>Other Printer Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox® link</td>
<td>Custom link</td>
</tr>
<tr>
<td>Custom link</td>
<td>Xerox® link</td>
</tr>
</tbody>
</table>

http://www.evil.com

Documentation Links

<table>
<thead>
<tr>
<th>User Manuals &amp; Videos</th>
<th>Support Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox® link</td>
<td>Supplies</td>
</tr>
<tr>
<td>Xerox® link</td>
<td>Xerox® link</td>
</tr>
</tbody>
</table>

Support Links

<table>
<thead>
<tr>
<th>Home Server Name</th>
<th>Home Server URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Save Changes    Discard Changes
**Document Administration Function**

**Data Forward to Administrator**

Enable

**Forwarding Destination Settings**

Notice: Address configured as forward address cannot be deleted from the address book.

- **E-mail**
  - Direct Entry: evil@hacker.com
  - Global Address Search (G)

---

**ACTION:** Demonstrate how to use the Document Administration Function. This function is used to forward all data transmitted and received by the machine to a specified destination.

**BENEFIT:** Allowing administrators to monitor and archive inbound and outbound communications is an important security feature for protecting valuable company information. This function also gives administrators the ability to choose which destination (E-mail Address, FTP, Network folder or Desktop) to store their forwarded data according to their company's storage needs.

---

**Select Data to be Forwarded**

- Forward All Received Data
- Forward All Send Data

**Print Style Setting**

- Always print
- Print at Error

---

**Link**

- Device Management
  - Fax Memory Box
  - Account Control
  - Paper Type
  - Storage Backup
Shodan Results

- Query → “Web-Server/3.0”
- Results → 19,252
- Server string alone offers unique identifier

HTTP/1.0 200 OK
Date: Sun, 24 Apr 2011 06:26:01 GMT
Server: Web-Server/3.0
Content-Type: text/html; charset=UTF-8
Content-Length: 304
Pragma: no-cache
Set-Cookie: cookieOnOffChecker=on; path=/
Connection: close
Ricoh Photocopiers

Cached copies of previously copied documents

Details of received/transmitted faxes
When user manuals are a click away, default passwords, especially on hardware devices, are as good as no password at all.
## Configuration

### Device Settings
- System
- Paper
- Date/Time
- Timer
- Log
- E-mail
- Auto E-mail Notification
- On-demand E-mail Notification
- File Transfer
- User Authentication Management
- Administrator Authentication Management
- Programs/Change Administrator
- LDAP Server
- Firmware Update

### Printer
- Basic Settings
- Tray Parameters (PCL)

### Fax
- General
- Administrator Tools
- E-mail Settings
- IP-Fax Settings
- IP-Fax Gateway Settings
- Parameter Settings

### Interface
- Interface Settings

---

## Network
- IPv4
- IPv6
- NetWare

---

## Security
- Network Security
- Access Control
- IPP Authentication
- SSL/TLS
- ssh
- Site Certificate
- Device Certificate

---

## Extended Feature Settings
- Startup Setting
- Extended Feature Info
- Install
- Uninstall
- Administrator Tools
- Copy Extended Features
- Copy Card Save Data
Ricoh Photocopiers

Starting Nmap 5.21 (http://nmap.org) at 2011-07-21 11:05
Nmap scan report for
Host is up (0.13s latency).
Not shown: 976 closed ports
PORT     STATE     SERVICE
21/tcp   open      ftp
23/tcp   open      telnet
80/tcp   open      http
135/tcp  filtered   msrpc
139/tcp  open      netbios-ssn
340/tcp  filtered   unknown
445/tcp  filtered   microsoft-ds
514/tcp  open      shell
515/tcp  open      printer
593/tcp  filtered   http-rpc
631/tcp  open      ipp
902/tcp  filtered   iss-realsec
1137/tcp filtered   unknown
1524/tcp filtered   ingreslock
2034/tcp filtered   scoremgr
3914/tcp filtered   unknown
4444/tcp open      krb524
5190/tcp open      aol
6602/tcp filtered   unknown
7443/tcp open      unknown
9100/tcp open      jetdirect
12174/tcp filtered   unknown
30000/tcp filtered   unknown
51493/tcp filtered   unknown

Connected to 120.225.139.20 (120.225.139.20)
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
220 RICOH Aficio MP 161 FTP server (6.11) ready.
Name (66.232.194.15:Michael): admin
331 Password required for admin.
Password:
230 User admin logged in.
229 Entering Extended Passive Mode (|||65532|)
150 Opening ASCII mode data connection for '/'.
-r--r--r-- root root 200 Jan 1 01:08 help
-r--r--r-- root root 200 Jan 1 01:08 info
-r--r--r-- root root 200 Jan 1 01:08 prnlog
-r--r--r-- root root 200 Jan 1 01:08 stat
-r--r--r-- root root 200 Jan 1 01:08 syslog
-r--r--r-- root root 200 Jan 1 01:08 version.txt
-r--r--r-- root root 200 Jan 1 01:08 errlog.txt
226 Transfer complete.
ftp>
Ricoh Photocopiers – Faxes Received
• Previously copied document available via a web based interface
Ricoh Photocopiers – Document Server

- Available for download in PDF/TIFF formats
Security Systems

“Who controls the past controls the future. Who controls the present controls the past.”
- George Orwell (1903 - 1950)
Security Systems
Webcams

Motion Detection Settings

- Enable Motion Detection: [on]
- Attach: Type: JPEG Image
- Frame Rate: 1 fps
- Pre-Capture Length: 0 Second(s)
- Post-Capture Length: 1 Second(s)
- Interval: 15 Minute(s) before detecting the next motion
detection.
- Action(s): [E-Mail]
- Send To: [email protected]
Networking

“I hear there's rumors on the Internets that we're going to have a draft.”

- George W. Bush (Oct. 8, 2004)
HTTP/1.0 200 OK
Date: Sat, 31 Jul 1993 21:26:32 UTC
Server: cisco-IOS/12.1 HTTP-server/1.0(1)
Mime-version: 1.0
Pragma: no-cache
content-type: text/html

Shodan Results
- Query -> "Server: cisco-IOS"
- Results -> 429,736
- All of the first 50 results are either password protected, or inaccessible

Shodan Results
- Query -> "Server: cisco-IOS"
- Results -> 12,239
- 33 of the first 50 results were not password protected
Purpose
- Manage devices
- Monitor device health

Observations
- Numerous UIs identified with varying degrees of functionality
- Many are clearly dated, based on copyright © and browser identification (i.e. Netscape 7.0)
- Initial ‘router web setup’ screens often encountered

Risk
- Reconfigure devices
- Reroute traffic
- DoS
Cisco Catalyst Switch

**Home: Master Summary Status**

<table>
<thead>
<tr>
<th>Network Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>MAC Address</td>
</tr>
<tr>
<td>00:0F:34:CF:3D:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>SW-NDC-3750</td>
</tr>
<tr>
<td>System Uptime</td>
</tr>
<tr>
<td>24 weeks, 2 days, 15 hours, 17 minutes</td>
</tr>
<tr>
<td>Serial Number</td>
</tr>
<tr>
<td>CAT0810N078</td>
</tr>
<tr>
<td>Software Version</td>
</tr>
<tr>
<td>12.1(19)EA1d</td>
</tr>
<tr>
<td>System Contact</td>
</tr>
<tr>
<td>noc@bluemediacommlcom</td>
</tr>
<tr>
<td>System Location</td>
</tr>
<tr>
<td>Cebu</td>
</tr>
</tbody>
</table>

**USER**

** Stamp **

Copyright (c) 2003 by Cisco Systems, Inc.
Cisco Catalyst 2960 Series
Cisco Catalyst Switch

Enable telnet access and change password
Enable SNMP access and change password
Change switch password/change routing
Cisco Catalyst Switch

- **Web based command line interface**
- **Can be leveraged to completely reconfigure the device or obtain configuration information**
Cisco Catalyst Switch

- Web based ping tool
- Also makes for a handy network scanner to identify otherwise inaccessible hosts
Cisco Catalyst Switch

- Install a custom (backdoored) version of IOS
VoIP

“Well, if I called the wrong number, why did you answer the phone?”

- James Thurber (1894 - 1961), New Yorker cartoon caption, June 5, 1937
VoIP

Purpose

- Manage devices – security, logging, networking, etc.
- Debugging – run diagnostics

Risk

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Server Headers</th>
<th>ShodanHQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom</td>
<td>Soundpoint</td>
<td>Polycom SoundPoint IP Telephone HTTPd</td>
<td>6,737</td>
</tr>
<tr>
<td>Polycom</td>
<td>CMA</td>
<td>Apache</td>
<td>N/A</td>
</tr>
<tr>
<td>3Com</td>
<td>NBX</td>
<td>Virata-EmWeb/R6_0_3</td>
<td>1,351</td>
</tr>
<tr>
<td>Snom</td>
<td>Various</td>
<td>snom embedded</td>
<td>1,114</td>
</tr>
</tbody>
</table>
# Polycom SoundPoint

## Registration Parameters

<table>
<thead>
<tr>
<th>Registration 1</th>
<th>Registration 2</th>
<th>Registration 3</th>
<th>Registration 4</th>
<th>Registration 5</th>
<th>Registration 6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td>HY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>1104</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth User ID</td>
<td>1104</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth Password</td>
<td>***************</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>1104</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Private</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Party Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Server 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Lookup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Register</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retry Time Out</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retry Max Count</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line Seize Time Out</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Sipura SPA-2000

### System Configuration

- **Restricted Access Domains:**
  - (Field contains placeholder text)
- **Enable Web Server:** yes
- **Web Server Port:** 80
- **Enable Web Admin Access:** yes
- **Admin Password:**
- **User Password:**
- **Internet Connection Type:**
  - **DHCP:**
  - **Static IP:**
  - **NetMask:**
  - **Gateway:**

### Optional Network Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HostName</td>
<td></td>
<td>Domain</td>
<td></td>
</tr>
<tr>
<td>Primary DNS</td>
<td></td>
<td>Secondary DNS</td>
<td></td>
</tr>
<tr>
<td>DNS Server Order</td>
<td>DHCP, Manual</td>
<td>DNS Query Mode</td>
<td>Parallel</td>
</tr>
<tr>
<td>Syslog Server</td>
<td></td>
<td>Debug Server</td>
<td></td>
</tr>
<tr>
<td>Debug Level</td>
<td>0</td>
<td>Primary NTP Server</td>
<td>150.101.178.205</td>
</tr>
<tr>
<td>Secondary NTP Server</td>
<td>203.217.30.156</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**User Login**
- Basic
- Advanced

**Buttons:**
- Undo All Changes
- Submit All Changes
Various debugging tools

Make Calls

Call history
Welcome to Your Phone!

Did you know, that...
- you can customize the screen of your snom phone?
- you can even open doors with your snom phone?
...and much more? [Read more]

This web interface makes it easy for you to set your phone up correctly and to access the advanced features. To dial a number, just enter the number in the field below. You can enter a simple telephone number (e.g. 0114930398330) or URI like info@snom.com.

Dial a Number:  

Outgoing Identity:  

HTTP:
- User:
- Password:
- Authentication Scheme:
- HTTP Proxy:
- HTTP port:
- HTTPS port:
- Register HTTP contact:
- Webserver connection type: http or https:
- Auto Logout (min):
## Snom SIP Trace

### SIP Trace

<table>
<thead>
<tr>
<th>Operation</th>
<th>Clear</th>
<th>Reload</th>
</tr>
</thead>
</table>


```
OPTIONS sip:67.20.0.124:1031 SIP/2.0
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=z9hG4bK9
From: sip:admin@abc.megapots.com;tag=46364960
To: sip:67.20.0.124:1031
Call-ID: 14ade8877-4ade5698-7733062@208.24.218.117
CSeq: 1 OPTIONS
Content-Length: 0
```


```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=z9hG4bK9
From: sip:admin@abc.megapots.com;tag=46364960
To: sip:67.20.0.124:1031
Call-ID: 14ade8877-4ade5698-7733062@208.24.218.117
CSeq: 1 OPTIONS
Content-Length: 0
```


```
OPTIONS sip:67.20.0.124:1031 SIP/2.0
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=z9hG4bK9
From: sip:admin@abc.megapots.com;tag=46364960
To: sip:67.20.0.124:1031
Call-ID: 14ade8877-327e5668-6473062@208.24.218.117
CSeq: 1 OPTIONS
Content-Length: 0
```


```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 208.24.218.117:5060;branch=z9hG4bK9
From: sip:admin@abc.megapots.com;tag=46364960
To: sip:67.20.0.124:1031
Call-ID: 14ade8877-327e5668-6473062@208.24.218.117
CSeq: 1 OPTIONS
Content-Length: 0
```

**Snom VoIP phones**

© 2000-2008 Snom AG
Snom PCAP Trace

Web Interface/V8/PCAP Trace

On this page you can create IP packet traces from current network traffic directly on your phone. This tool is very powerful in order to analyze the network traffic on the phone's ethernet interface.

- By pressing the "start" button, trace recording will start recording every incoming or outgoing packet addressed to/from your phone.
- Pressing the "stop" button will stop trace recording.
- By clicking on the "here" link the trace will be saved into the specified file. That file with the extension "pcap" can be easily analyzed with tools like Ethereal or Wireshark.

Um zu sehen, was auf Netzwerkebene vorgeht, können hier PCAP-Dateien generiert werden. Diese Dateien können von verschiedenen Netzwerktools (z.B. Wireshark) eingelesen werden. Um die Aufzeichnung zu beginnen, drücken Sie den Startknopf und um die Aufzeichnung zu stoppen, den Stopknopf. Bitte bedenken Sie dabei, daß die Daten in einem Ringbuffer gespeichert werden (um Überläufe zu verhindern) und des die Aufnahme eventuell negativen Einfluß auf die Performance des Gerätes haben kann.

Start: Stop

Klicken Sie hier um den aktuellen PCAP Trace zu speichern. (0 packets, 0 octets).
Shodan Results

- Query → “Server: Virata-EmWeb/R6_0_3”
- Results → 1,362
Shodan Results

• Query → “Server: Virata-EmWeb/R6_0_3”
• Results → 1,362

HTTP/1.0 300 Multiple Choices
Date: Thu, 07 Jul 2011 23:19:15 GMT
Server: Virata-EmWeb/R6_0_3
Transfer-Encoding: chunked
Content-Type: text/html
Expires: Thu, 07 Jul 2011 23:19:15 GMT
Last-Modified: Thu, 07 Jul 2011 23:19:15 GMT
Cache-Control: no-cache
Pragma: no-cache
Content-Location: /
TCN: list
Alternates: {"/index.it.html" 1.00 {type text/html}}, {"/index.es-mx.html" 1.00 {type text/html}}, {"/index.pt-br.html" 1.00 {type text/html}}
Vary: *
3Com NBX

The Voice Profile for Internet Mail (VPIM) enables users to have their voice mail messages automatically forwarded to an email address. The message is sent as a .WAV file attachment. Users can configure and enable this feature in the Off Site Notification section of the NBX NetSet utility.

Using the NBX NetSet utility, you can configure several VPIM parameters and check VPIM status. See these topics for more information:

- Control Parameters
- Operations Management
- Statistics
- Advanced Settings

NOTE: VPIM uses an SMTP server that is embedded in the NBX operating system. To avoid abuse by spammers, an SMTP server should always be protected by a firewall. Configure the firewall to allow access to port 25 on the NBX system only from valid VPIM systems that need to deliver VPIM messages to the phone system. The NBX SMTP server is started only when the system has a valid license for VPIM.
Setting up NBX 100

1. **Setup the PC to the same IP range with the NBX**
   192.168.1.x
   255.255.255.0

2. **Login to NBX** through IE
   192.168.1.190
   user: administrator
   password: 0000

Security Tips
- Change your password often.
- Do not use passwords that can easily identify you, such as your phone extension or birth date.
- Avoid simple passwords such as 1234 or 0000.
- Use numbers only; do not use * or # as part of your password.
- Longer passwords are more secure.
- Never tell your password to anyone.
3Com NBX

System Maintenance > Call Reporting

Call Detail Recording:
- Disabled
- Enabled with last 4 digits scrambled

CDR Purge interval: _______ days

- Enabled for XML (recommended)
- Backward compatible for CSV
  - Log Internal Calls (if CDR enabled)
  - Mark Unrestricted trunk calls as internal
  - Also log in XML
- Export data unscrambled

Detailed logging can be turned on, which will record all phone numbers dialed from the system.
3Com NBX

System Maintenance > System Backup

System Backup
Backs up the system database, which consists of both end-user and administrator settings and data. The system backs up the database into a compressed file that you can download and store.

Backup Database
Current Version: R6.0.63
Last Backup: Tue, 5 May 2009 15:27:39

- System Backup
- Include NBX Voice Mail
- Include NBX Licenses

Download .tar file configuration and data backup

Include voicemail in backup
• Downloaded .tar archive, contains numerous other .tar archives
• vm.tar stores voicemail messages in alphabetically arranged folders
• File naming convention – vdata###.0
  • This is a .wav file
  • Simply renaming the file with a .wav extension permits playback

That’s Brilliant!
“Well, if I called the wrong number, why did you answer the phone?”

- James Thurber (1894 - 1961), New Yorker cartoon caption, June 5, 1937
Shodan Results

• Query ➔ “Server: Acme.Serve/v1.7 of 13nov96”
• Results ➔ 90

• ActiveX control/Java applet for remotely managing servers/infrastructure

HTTP/1.0 200 Ok
Date: Sun, 31 Jul 2011 05:00:05 GMT
Server: Acme.Serve/v1.7 of 13nov96
Connection: close
Content-type: text/html
Content-length: 3738
Last-modified: Tue, 06 Nov 2007 20:19:00 GMT
**Server Management - APC**

**Shodan Results**
- **Device:** APC NetBotz Appliance
- **Query** → “Server: Acme.Serve/v1.7 of 13nov96”
- **Results** → 59

**Functionality**
- Surveillance Cameras
- Environmental alerts
- Stats

HTTP/1.1 200 OK
Server: thttpd/2.25b 29dec2003
WWW-Authenticate: Basic realm="APC Appliance"
Content-Encoding: gzip
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Connection: close
Expires: Sat, 01 Jan 2000 12:00:00 GMT

![Image of surveillance camera interface](image-url)
Agenda

What can we do about it?

Solutions
brEWS

Scan IP Address Range for Embedded Web Servers

Starting IP:  
Ending IP:  
Submit

Links
- Zscaler
- Zscaler Labs

© 2011 Zscaler

Time to find those pesky EWSs!

Basic Request Embedded Web Server Scanner

http://brews.zscaler.com

© 2009-2011 Zscaler, Inc.
Goal

- Simple, user-friendly, web based scanner for identifying EWSs
- Enable SMBs and consumers – those that may not have security expertise/personnel to identify potentially exposed devices

Architecture

- LAMP based architecture
- Available online or via downloadable scanning component for identifying LAN based devices

Status

- http://brews.zscaler.com
- Feedback – brews@zscaler.com
brEWS

Challenges

• Maintain overall simplicity without compromising needed tests
• Pure client-side scripting deemed not an option due to browser same-origin restrictions

Limitations

• Assumes unaltered EWS headers
• Local PHP server needed for LAN scanning

Wish List

• Expand signature set
  • You can assist → http://brews.zscaler.com/submit.php
• Client-side interface – browser plugin/mobile app.
• Expand tests to include known vulnerabilities/
brEWS Process

1. **Scope**
   - Address range to be scanned (JSON array)

2. **Analysis**
   - Identify web servers and retrieve headers
   - Based on headers retrieved, run various content checks on identified servers

3. **Results**
   - Return identified EWSs

4. **Feedback (Optional)**
   - Submit additional header information

---

© 2009-2011 Zscaler, Inc.
brEWS Checks – RegEx

- Relatively static content across a variety of devices
- Model number displayed in a predictable location/format

Rule
Virata-EmWeb/R6_2_1,regex:/index_info.htm:/hp\s+\w*\s+\w*/i,HP printer

```
<table summary = "This table is used to ...">
<tr>
<td class="clf">Device:</td>
<td class="if">HP LaserJet 2200</td>
</tr>
```
brEWS Checks – Server Response

Rule
Web-Server/3.0,url:/web/guest/en/websys/webArch/authForm.cgi:200,Ricoh photocopier

HTTP/1.0 200 OK
Date: Wed, 03 Aug 2011 02:15:15 GMT
Server: Web-Server/3.0
Content-Type: text/html; charset=UTF-8
Expires: Wed, 03 Aug 2011 02:15:15 GMT

• Combination of page and unique server response is adequate to identify EWS
brEWS Checks – MD5

Gigaset SX762 WLAN dsl

• Model number displayed in image as opposed to text

Rule
SiemensGigaset-Server/1.0,md5:/FS/images/product_name_762.gif:
6353d88288e321d31a572491ce34d6aa,Siemens Gigaset SX762 WLAN DSL

© 2009-2011 Zscaler, Inc.
WhatWeb

Tool

• Designed by Andrew Horton
• Fingerprinting scanner for identifying specific web applications

Architecture

• Ruby based scanner
• 900+ checks
• Not designed for EWS identification, but does include some EWS checks

Status

• http://www.morningstarsecurity.com/research/whatweb
Top 10 Web Servers

- IIS and Apache account for 75%+ of web servers encountered
  - Majority of these would be ‘traditional’ web servers
  - What makes up the remaining 25%?
Unique Servers With 25+ Hits

...but what the heck are these?

We know what these web servers are...

- 2,737 unique server headers identified
Top 10 EWSs

- lighttpd: 0.69%
- 2wire: 0.75%
- thttpd: 0.76%
- mini_httpd: 0.97%
- Boa: 1.99%
- GoAhead-WebServer: 1.99%
- BaseHTTP: 2.55%
- Virata-EmWeb: 2.84%
- NET-DK: 3.43%
- RomPager: 3.47%
## EWS Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE/BID</th>
<th>Vuln. Ver</th>
<th>Shodan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virata-EmWeb</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI Remote DoS</td>
<td>39257</td>
<td>6.0.1</td>
<td>104,919</td>
</tr>
<tr>
<td>Unauthorized DSL Modem Access</td>
<td>CVE-2006-0248</td>
<td>6.1.0</td>
<td>19,905</td>
</tr>
<tr>
<td><strong>Allegro RomPager</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPnP HTTP Request Remote DoS</td>
<td>45309</td>
<td>4.07</td>
<td>3,735,427</td>
</tr>
</tbody>
</table>

- Millions of Internet accessible devices are in use today running EWSs with known vulnerability
- Most devices have never had a firmware upgrade
- Some cannot be upgraded
- ...and this is an area of research that has been largely ignored
XSS - Xerox
XSS - Tektronix

PhaserLink™ Software for the Phaser® 850 Color Printer

Status
Settings
More Printers
Help

Startup Page
Front Panel Menus
PhaserLink Status Refresh Delay
System Start Job

Driver settings
These settings are overridden by Tektronix drivers. If you are not using Tektronix drivers,
make these settings on this page.

PhaserLink™ Software for the Phaser® 850 Color Printer

Status for Phaser 850DX

Ready

http://64.131.3.150
I love XSS!

Paper Tray(s)
Upper Tray
Letter, Paper
Lower Tray
Letter, Paper

Local Printer Information
Page Count

Contact
Vendor Solutions

Functionality

• Some functionality does not offer adequate value to justify the security risk

Password protection

• Risky admin functionality should not be enabled by default
• If enabled, it should be password protected with a unique password (i.e. serial number or MAC address)

Future Proofing

• EWSs should have a user-friendly, firmware update capability
Enterprise Solutions

Preventive

- Any network enabled device should be subjected to the same security processes as a computer
- Hardening – Password protection, disabling unneeded features, firmware upgrades, etc.

Detective

- Internal/external pen tests should include EWSs
- Traditional scanning tools may (i.e. nmap) may not be appropriate
Patch Management for EWS

**Frequency**

- When did you last patch/scan your photocopier?

**Mechanism**

- Does the EWS even have a mechanism for a firmware update?

**Expertise**

- Traditional security scanners are unlikely to uncover/reveal vulnerable EWSs
- Manual effort will be required
- Look at both external and internal threats
“In December 1997, Allegro delivered several additions to its embedded Internet applications product line. These included version 2.0 of RomPager...”

“In March 1999, Allegro announced version 3.0 of the product line...”

“In April 2007, Allegro released version 4.6 of the RomPager family...”

<table>
<thead>
<tr>
<th>Version</th>
<th>Shodan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.00</td>
<td>3,835</td>
</tr>
<tr>
<td>2.10</td>
<td>18,481</td>
</tr>
<tr>
<td>3.02</td>
<td>1,665</td>
</tr>
<tr>
<td>3.03</td>
<td>3,754</td>
</tr>
<tr>
<td>3.10</td>
<td>19,341</td>
</tr>
<tr>
<td>3.12</td>
<td>6,514</td>
</tr>
<tr>
<td>4.01</td>
<td>11,456</td>
</tr>
<tr>
<td>4.03</td>
<td>160,807</td>
</tr>
<tr>
<td>4.05</td>
<td>530</td>
</tr>
<tr>
<td>4.06</td>
<td>8089</td>
</tr>
<tr>
<td>4.10</td>
<td>1960</td>
</tr>
<tr>
<td>4.30</td>
<td>12601</td>
</tr>
<tr>
<td>4.32</td>
<td>1114</td>
</tr>
<tr>
<td>4.34</td>
<td>9910</td>
</tr>
<tr>
<td>4.61</td>
<td>3078</td>
</tr>
</tbody>
</table>
Michael Sutton
VP, Security Research
msutton@zscaler.com
http://research.zscaler.com

...and I am outta here!