CPE Security

Warren Kumari

Apologies…

- Apologies to Ondrej Filip, these are general issues. These do not apply to Turris…
- Which I run at home, and it doesn't suck.
- He can probably provide more details on the issues.

CPE

- Customer Premises Equipment
- Things like Netgear, Linksys, D-Link, Belkin, Adtran, Edimax, Mikrotik, Motorola, Nortel, Actiontec, SMC, Cisco, Westell, ZOOM, ZyXEL, ASUS…
- The widget that connects your house to the [Cable|DSL|WISP|Satellite|Internet]

CPE (cont)

- Incredibly thin margins… like pennies…
  - Device manufactured by cheapest vendor
  - Using highly integrated CPUs
    - Closed libraries, under NDA, binary blobs
  - CPE Vendor -> Outsourcer -> Hardware vendor -> Software vendor
    - Outsourcer takes Linux (or ZynOs, or similar), DNSMasq (or similar), web server (of sorts), TR-069 code, TR-xxx, SNMPd (or ..

CPE (cont.)

ZyXEL MWR102 Wireless Router - 150 Mbps - 2.4 GHz - 802.11b/g/n

Linksys E4200 IEEE 802.11n Ethernet Wireless Router

$6.33 from 2 stores

NETGEAR | Netgear WNR1000-100NAS N150 Wireless Router

The WNR1000-100NAS N150 Wireless Router form Netgear® provides immense wireless coverage for your network. Also, this device gets an extra performance boost when connected to Wireless-N devices. You can now surf, ... Full Description

Market Value[1]	$44.99
Instant Savings	$20.00
Dell Price	$24.99

Add to Cart

Usually Ships: 24 Hours

Email to a Friend

Print-Friendly Version

What's in the Box

Click to Call

Manufacturer Part# : WNR1000-100NAS | Dell Part# : A2866576

Issues

- DNSChanger - 2007 - 2011 (Rove Digital)
  At its peak, DNSChanger was estimated to have infected over 4 million computers, bringing in at least US$14 million in profits to its operator from fraudulent advertising revenue.
- RomPager / Misfortune Cookie - 12million devices
  "at least 12 million readily exploitable devices connected to the Internet present in 189 countries across the globe"
- NetUSB (tcp/20005) (KCodes)
  Millions of devices, "20% of world's networking devices include KCodes technology", kernel vulnerability, ZyXEL will begin issuing firmware updates in June, while Netgear plans to start releasing patches in the third quarter of the year.
- TR-069; More than 60 undisclosed vulnerabilities affect 22 SOHO routers, etc…

Case study - ROMPager

- AKA Misfortune Cookie
- RomPager embedded web server version 4.07, released in 2002
- Alegro fixes issues in RomPager v4.34, 2005
  - Fix provided to *customers*
  - Currently v5.40.
- “In some cases, manufacturers continue to make and sell products with software components that are over 13 years old…”
- D-Link, Edimax, Huawei, TP-Link, ZTE, ZyXEL …

ROMPager

- No dynamic memory management
- Pre-allocated cookies array
  - 10 cookies, 40 bytes long each
    - C0,C1,C2,…,C9
    - Cookie: C0=43765EF342C125AC6;
- **Trivial** exploit
- Cookie: C107373883=/foo

IoT

- Latest sexy buzzword
  - ***EVERYTHING*** will have an IP address and be connected to the Internet.
- Once again, price is critical / margins are thin / tiny CPUs, tiny memory / time to market, etc.
- Issues for CPE == issues for IoT.

Root issues

- Once a product is shipped, there is no incentive to update it.
  - Negative incentive.
  - It's hard - vendor may not have ability to fix
    - No more contract with hardware vendor
    - Chipset no longer supported
    - No way to get fixes to users
    - No modular software - statically linked

Solutions?!

- Raising awareness of the issues.
  - Customers may start demanding better
- Regulation?! (Gulp!)
  - This will end poorly…
- Improve the toolset, libraries, etc
  - If you make it cheaper / easier / better…

Arduino as a model

```
/*
  Blink
  Turns on an LED o

  This example code
 */

// Pin 13 has an LE
// give it a name:
int led = 13;

// the setup routin
void setup() {
  // initialize the
  pinMode(led, OUTP
}

// the loop routine
void loop() {
  digitalWrite(led,
  delay(1000);
  digitalWrite(led,
  delay(1000);
}
```

Blink §

```
/*
  CoolBeans Router Model 42
  Best router, now with WiFi!
 */

#include <ipv4.h>
#include <ipv6.h>
#include <webserver.h>

#define NAME 'CoolBeans Router'
#define SERVICE_LIST D_WIFI|D_ETH|D_WEB|D_TR69

// Setup runs when the box is first installed, or reset.
void setup() {
  // delete the curret config, then run webserver.
  config(WRITE, "");
  webserver.run('/var/www/html/index.html');
}

// the loop function runs over and over again forever
void loop() {
  process_packet();
  process_WiFi();
  blink();
}
```

Questions?