CSIRT.SK
www.csirt.gov.sk

Zraniteľnosti domácich smerovačov

Valéria Harvanová

Konferencia INFORMAČNÁ BEZPEČNOSŤ 2017

Agenda

- architektúra domácich “wifi” sietí
- smerovač Ubee EVW3226 a jeho zraniteľnosti
- príklad útokov
- dopady

Typická domáca sieť

Bezpečnosť architektúry

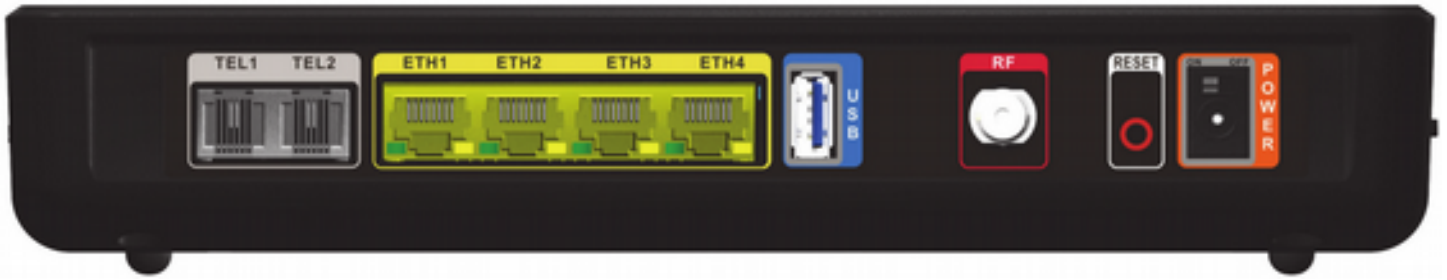
- kompromitácie zariadenia → L2 dosah na zvyšok siete
- znalosť PSK → L2 dosah na zvyšok siete
- kompromitácia smerovača → odpočúvanie komunikácie LAN ↔ Internet

=> bezpečnosť LAN je závislá na bezpečnosti smerovača (najmä jeho firmvéru a konfigurácie)

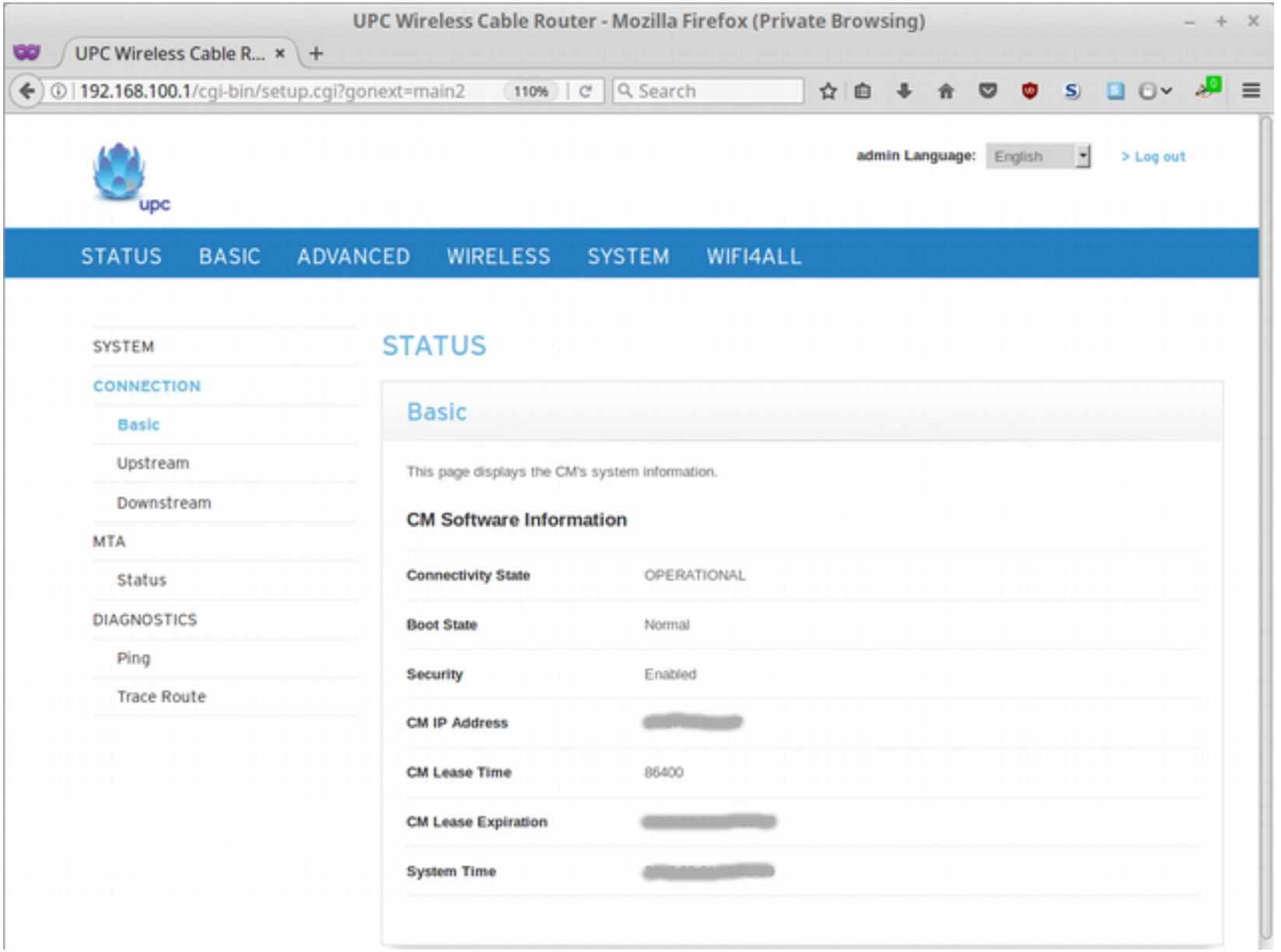
Ubee EVW3226 (1)

- rozšírený smerovač poskytovaný slovenským ISP (ako jeden zo 4 modelov)
- firmvér/sofvér aj aktualizácie spravované operátorom
- 4 LAN porty, 1 USB rozhranie, 2.4/5 GHZ “wifi”
- EuroDOCSIS 3.0 cable
- OS Linux
- správcovské webrozhranie

Ubee EVW3226 (2)



Ubee EVW3226 (3)



Testovanie zraniteľností

- Jún/júl 2016 (niektorí iní analytici skôr)
- Testovaná verzia SW: EVW3226_1.0.20
- Aktuálna verzia SW: EVW3226_2.07b
- Testovali:
  - SEARCH-LAB Ltd.
  - SEC Consult Vulnerability Lab
  - blog 0xDEADC0DE
  - Firefart
  - CSIRT.SK

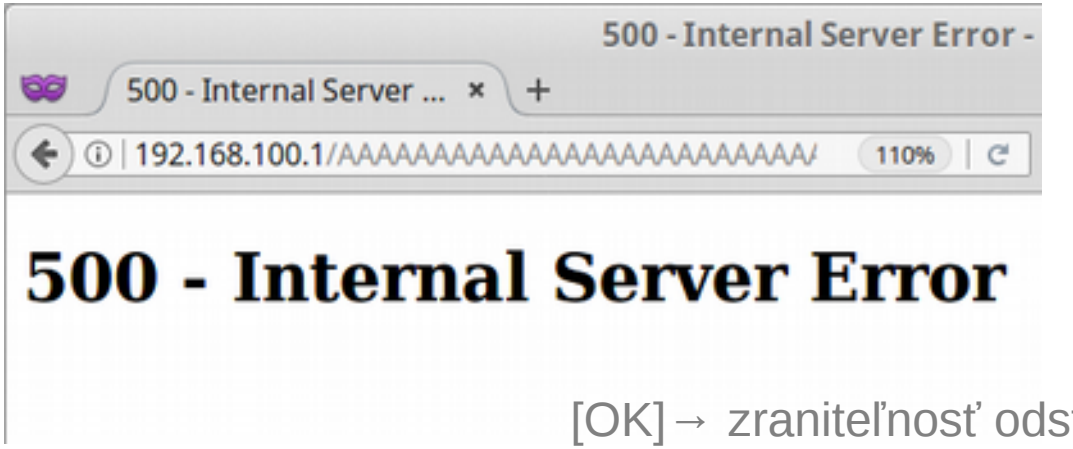
Zraniteľnosti správcovského webrozhrania (1)

- zadné vrátka [OK]
  - `http://{ip.addr}/cgi-bin/setup.cgi?` **`factoryBypass=1`**
- prístupná záloha konfigurácie bez autentifikácie [OK]
  - `http://{ip.addr}/Configuration_file.cfg`
  - chránená heslom → slovníkový útok / RE
- manažment relácie na základe zdrojovej IP adresy [X]
  - **192.168.0.2xy**

[OK] → zraniteľnosť odstránená
[X] → zraniteľnosť pretrváva

Zraniteľnosti správcovského webrozhrania (2)

- webrozhranie prístupné len cez HTTP [X]
- nedostatočne kontrolované používateľské vstupy – buffer overflow [X]
  - `http://{ip.addr}/{254+ znakov}.cfg`



[OK] → zraniteľnosť odstránená
[X] → zraniteľnosť pretrváva

Nebezpečné východzie nastavenia

- rovnaký prednastavený používateľ `admin:admin` [X]
- WPA2-Personal so slabým PSK [X]
  - ESSID UPC1234567
  - PSK WAVALBAG

    // 8 * veľké písmeno → kompexita 26^8 ≈ 2^38
  - PSK závisí od ESSID a BSSID

[OK] → zraniteľnosť odstránená
[X] → zraniteľnosť pretrváva

Nedokumentované správcovské rozhranie

- CLI (/bin/sh) cez Telnet (TCP/23) [OK]
  - `admin:admin` (UID 0)
  - `root:pega#123` (UID 0)
- webrozhranie na http://192.168.100.1 [X]

```
rndbr1    inet addr:192.168.0.1  Mask:255.255.255.0
rndbr1:1 inet addr:192.168.100.1  Mask:255.255.255.0
```

[OK] → zraniteľnosť odstránená
[X] → zraniteľnosť pretrváva

Fyzická bezpečnosť

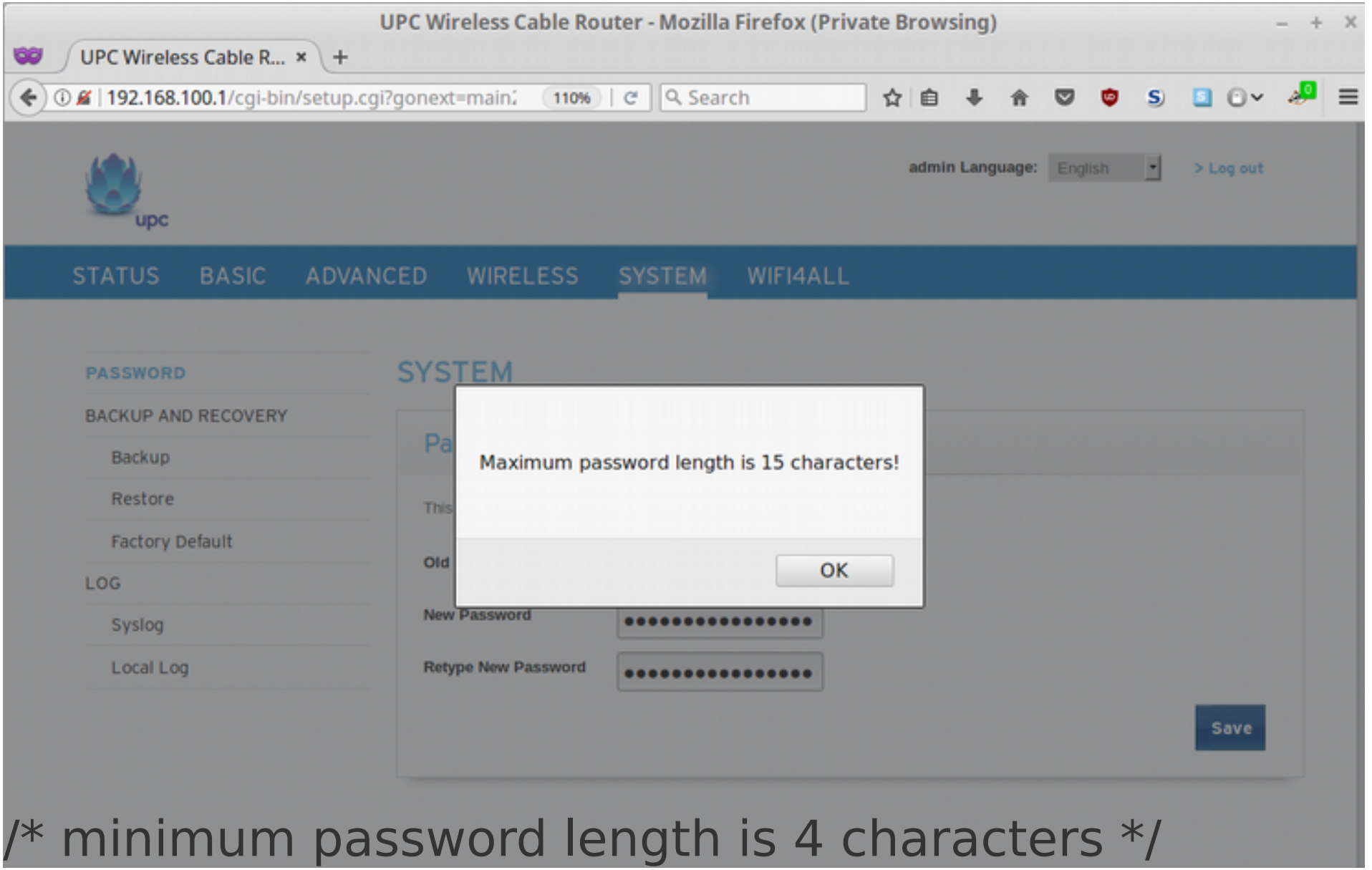
/* nami neoverené */

- USB kľúč s konkrétnym názvom + .auto skript
- UART rozhranie s prístupom na shell (s potrebou autentifikácie)

Procesy operátora

- viaceré zraniteľnosti → nedokonalý proces hodnotenia zabezpečenia a zraniteľností
- aktualizácia v lete 2016 → aktualizácie môžu viesť k zavedeniu zraniteľností
- odstraňovanie zraniteľností a notifikovanie používateľov → nedostatky v procese odstraňovania ohlásených zraniteľností
- nie je k dispozícii návod na hardenovanie zariadení a LAN

“Maximum password length is 15 characters!”



/* minimum password length is 4 characters */

Príklady útokov a dopady (1)

- skenovanie siete a hľadanie ESSID UPC1234567
- dopočítanie PSK a pripojenie k sieti

- náročnosť útoku: nízka
- dopad: L2 prístup k sieti a prístup do Internetu

Príklady útokov a dopady (2)

/* Útočník má prístup do siete: */

- Pripojenie na smerovač cez Telnet
- odpočúvanie komunikácie prostredníctvom štandardných linuxových nástrojov

- náročnosť útoku: nízka
- dopad: determinácia spojení, čítanie nešifrovanej komunikácie, ...

Príklady útokov a dopady (3)

/* Útočník má prístup do siete: */

- autentifikácia na webrozhranie (factoryBypass / východzie meno a heslo / iné)
- zmena DNS serverov → presmerovanie používateľov na škodlivé stránky

- náročnosť útoku: nízka
- dopad: možná kompromitácia ostatných zariadení v sieti

Odstraňovanie zraniteľností

- časť zraniteľností bola inými týmami ohlásená a konzultovaná s Liberty Global, Ubee, UPC Magyarorszag (už od roku 2015)
- 7-8.2016 – komunikácia CSIRT.SK s UPC Slovakia
- medzi augustom 2016 a februárom 2017 bola odstránená časť zraniteľností tichou aktualizáciou softvéru (UPC Slovakia)

Pôvod zraniteľností

- pri tvorbe firmvéru sa v dostatočnej miere nedbá na bezpečnosť návrhu a produktu
- ohodnotenia zabezpečenia a zraniteľností produktu nie sú vykonávané v potrebnom rozsahu
  - pri zavádzaní produktu do portfólia ISP
  - pri pridávaní/zmenách funkcionality

/* netýka sa to iba domácich smerovačov */

Záver

- domáci smerovač je typicky *single point of failure*
  - jeho kompromitácia znamená kompromitáciu celej siete
  - potreba dôkladného hardeningu
- z pohľadu používania pracovných zariadení je domáca sieť ekvivalentom verejnej siete
  - potreba VPN (aj pre DNS)

Otázky?

Zraniteľnosti domácich smerovačov

valeria.harvanova@csirt.sk