Zraniteľnosti domácich smerovačov

Valéria Harvanová
Špecializovaný útvar CSIRT.SK
DataCentrum
Cintorínska 5, 81108 Bratislava
e-mail:valeria.harvanova@csirt.sk

Abstrakt

The security of home network depends heavily on the security and resiliency of a home router that manages local network and provides connectivity to the Internet. If the router is compromised, whole network is compromised. This paper describes multiple vulnerabilities found on router Ubee EVW2336 that is used in many home networks in Slovakia. Exploitation of these vulnerabilities allowed to gain superuser shell access to the router, access to the administrative web interface and access to a local wireless network. Described vulnerabilities are a subset of vulnerabilities found by SEARCH-LAB Ltd., SEC Consult Vulnerability Lab, 0xDEADC0E and CSIRT.SK.

1. Typická konfigurácia domácej siete

Slovenské domácnosti sa do Internetu pripájajú typicky nasledujúcim spôsobom. Domáci smerovač je prenajatý alebo kúpený od poskytovateľa pripojenia do Internetu spolu s mesačným programom pripojenia do Internetu. Jedno rozhranie je pripojené do siete operátora a prostredníctvom toho do siete Internet. Na strane lokálnej siete (ďalej v texte LAN) sú typicky jedno alebo dve rozhrania bezdrôtovej siete (t.j. IEEE 802.11 - 2.4GHz alebo 5Ghz; ďalej v texte len „wifi“) a niekoľko Ethernet zásuviek. LAN je väčšinou tvorená jednou podsieťou, ktorá je od siete operátora oddelená len domácim routrom. Router funguje out-of-the-box, prípadne po vykonaní jednoduchého inicializačného postupu. Používateľ môže router čiastočne konfigurovať prostredníctvom administračného rozhrania - často je to obmedzené na nastavenia LAN, firewallu, použitých rekurzívnych DNS serverov a zmenu prihlasovacích údajov k správcovskému rozhraniu. Prístup do lokálnej siete cez „wifi“ je chránený prostredníctvom hesla (passphrase) a komunikácia je šifrovaná (WPA/WPA2-PSK)[1].

1.1. Potenciálne riziká a dôsledky

Pre opísanú konfiguráciu domácej siete platí, že ak sa útočníkovi podarí kompromitovať jedno zariadenie v LAN, tak má L2 dosah (t.j. na úrovni MAC adries) na všetky ostatné zariadenia v LAN, pričom tieto sú chránené len svojim lokálnym firewallom. Útočník môže kompromitované zariadenie využiť na ľubovoľnú činnosť – napríklad ako súčasť botnetu. *Na zamyslenie: ako je nastavený a je vôbec nastavený firewall vašeho mobilného telefónu, alebo vašej smartTV?*

[1]Niektoré domácnosti ešte stále používajú zabezpečenie WEP, ktorého bezpečnosť bola prelomená a považuje sa za zastarané a nebezpečné.

Ak sa útočníkovi (vo fyzickej blízkosti) podarí uhádnuť/dopočítať heslo (passphrase pre PSK), môže sa pripojiť do „wifi“ a teda do LAN a platia dôsledky z predošlého bodu.

Ak sa útočníkovi podarí kompromitovať router, má navyše aj dosah na komunikáciu medzi všetkými zariadeniami v LAN a Internetom. Môže tak útočiť na zariadenia v LAN, na služby v Internete, ku ktorým tieto zariadenia pristupujú, ako aj na akékoľvek iné zariadenia v Internete.

Pretože smerovač je zariadením v lokálnej sieti, ktoré sprostredkováva pripojenie do LAN aj do Internetu tak z vyššie uvedeného vyplýva, že bezpečnosť lokálnej siete bežnej slovenskej domácnosti je závislá od úrovne zabezpečenia tohto smerovača. Úroveň zabezpečenia smerovača závisí najmä od kvality firmvéru zariadenia a od bezpečného nastavenia jeho konfigurácie. O firmvér a východziu konfiguráciu zariadenia sa typicky stará dodávateľ / operátor a o konfiguráciu nastavení lokálnej siete sa stará zákazník.

Keďže smerovač funguje out-of-the-box, ponúka sa otázka: *Prečo by si zákazníci mali meniť správcovské meno a heslo alebo konfiguráciu zabezpečenia „wifi“ siete?* Testy ukazujú, že niektorí zákazníci to skutočne nerobia[2]. Tento prístup je z bezpečnostného hľadiska v poriadku za predpokladu, že východzia konfigurácia prenajatého zariadenia je dostatočne bezpečná. Teda okrem iného pre ňu platí nasledovné: 1) správcovský prístup je chránený silným heslom, ktoré je náhodne vygenerované pre daný router, 2) názov siete (ESSID) je unikátny a heslo (passphrase) je náhodne vygenerované a silné. Bod 2 je dôležitý vzhľadom na to, že

[2]Dokazuje to napríklad test dostupných wifi sietí v Bratislave z októbra 2016, ktorý ukazuje, že minimálne 5,98 % zachytených sietí malo ESSID predastavenom tvare a minimálne časť z toho mala aj pôvodné heslo (passphrase) [2]. Toto je len príklad na ilustráciu. Podiel takýchto zariadení je pravdepodobne vyšší.

protokol WPA/WPA2-PSK je zraniteľný na offline útok hrubou silou alebo slovníkový útok na hash[3], z ktorého sa dá odvodiť použité zdieľané tajomstvo.

Ako si ukážeme v ďalšej časti článku, spoliehať sa na bezpečnosť predvolených nastavení domáceho routra a na jeho celkovú bezpečnosť nemusí byť vhodné.

2. Zraniteľnosti domáceho smerovača Ubee EVW3226

Smerovač Ubee EVW3226 je zariadenie v minulosti dodávané slovenským poskytovateľom pripojenia do Internetu (ISP – ďalej v texte „operátor“) svojim zákazníkom. V súčasnosti je toto zariadenie stále podporované a rozšírené v domácnostiach zákazníkov. Smerovač má oficiálne dokumentované [1] správcovské webrozhranie, má 4 LAN porty, 1 USB rozhranie, podporuje 2.4GHz aj 5GHz „wifi“ a jeho firmvér ako aj aktualizácie sú pod správou operátora. Firmvér smerovača je postavený jadre Linux.

Zariadenie EVW3226 obsahovalo viaceré zraniteľnosti, z ktorých niektoré umožňovali získanie úplného prístupu k firmvéru zariadenia, respektíve získanie prístupu k webovému správcovskému rozhraniu. Verzia firmvéru nasadená na prenajímaných zariadeniach, ktorá je aktuálna ku dňu písania tohto článku[4] stále obsahuje niektoré pôvodne nájdené a operátorovi nahlásené zraniteľnosti.

2.1. Opis nájdených zraniteľností

Zraniteľnosti uvedené v tomto článku sú časťou súboru zraniteľností identifikovaných analytikmi zo SEARCH-LAB Ltd. [3], SEC Consult Vulnerability Lab [4], blogu 0xDEADC0E [5] a CSIRT.SK [6]. Napriek tomu, že sa jednalo o relatívne základné testy[5] na prítomnosť zraniteľností (angl. vulnerability assesment), tak bolo identifikovaných viacero závážnych zraniteľností. Je teda pravdepodobné, že zariadenie obsahuje aj ďalšie, nám aktuálne neznáme zraniteľnosti.

Zraniteľnosti správcovského webrozhrania

V správcovskom web rozhraní boli implementované zadné vrátka umožňujúce správcovský prístup bez znalosti používateľského mena a hesla. Jednalo sa o parameter `factoryBypass` skriptu setup.cgi. *[zraniteľný firmvér v. 1.0.20]* Po odoslaní nasledujúcich HTTP GET dotazov získal používateľ autentifikovanú reláciu:

```
http://{ip.addr}/cgi-bin/setup.cgi?factoryBypass=1
http://{ip.addr}/cgi-bin/setup.cgi?gonext=main2
```

[3]Potrebné údaje je možné zachytiť počas fázy autentifikácie legitímneho zariadenia pripájajúceho sa do danej siete (angl. 4-Way Handshake). Je nutná fyzická blízkosť útočníka.

[4]Firmvér verzie EVW3226_2.07b aktuálny ku dňu 27.2.2017.

[5]Testy nepokrývali celý „attack surface“– napr. neobsahovali komplexnú analýzu kódu firmvéru zariadenia.

Manažment relácie autentifikovaného používateľa je málo bezpečný. Autentifikovaný používateľ je identifikovaný len na základe zdrojovej IP adresy. Taktiež samotné overenie, či sa jedná o autentifikovanú zdrojovú IP adresu, je nesprávne – overuje sa iba prítomnosť reťazca známej IP adresy v reťazci zdrojovej IP adresy aktuálneho HTTP dotazu. Znamená to, že používateľ, ktorý sa autentifikuje napríklad z IP adresy 192.168.0.2 je automatický prihlásený aj z adries 192.168.0.2xy. *[zraniteľný firmvér v. 2.07b]*

Ak správca zariadenia spravil zálohu konfigurácie, tá bola prístupná na stiahnutie bez potreby autentifikácie cez statickú URL adresu až do reštartu zariadenia. Jednalo sa síce o súbor chránený heslom, no ten je možné podrobiť napríklad slovníkovému útoku (keďže heslo je špecifikované používateľom) alebo reverznému inžinierstvu. *[zraniteľný firmvér v. 1.0.20]*

Webová aplikácia neimplementuje v dostatočnej miere hardening voči štandardným útokom typu CSRF, Clickjacking a podobne. Webrozhranie je navyše prístupné len cez nešifrovaný protokol HTTP (port TCP/80). Táto skutočnosť zjednodušuje náročnosť zneužitia niektorých iných zraniteľností. *[zraniteľný firmvér v. 2.07b]*

Webová aplikácia nedostatočne kontroluje používateľské vstupy. Obsahuje viaceré zraniteľnosti typu pretečenie pamäti. Tieto môžu byť potenciálne zneužité k útoku, ktorého cieľom je vykonať ľubovoľný kód na zariadení.
Príklad zraniteľnosti: HTTP GET dotaz na `http://{ip.addr}/{254+ znakov}.cfg` vyvolá neošetrenú chybu na strane servera *[zraniteľný firmvér v. 2.07b]*

Nebezpečná out-of-the-box konfigurácia zariadenia

Prednastavený používateľ správcovského webrozhrania má pre všetky zariadenia tohto typu rovnaké a jednoduché prihlasovacie údaje: `admin:admin`.

Router má zapnutú „wifi“ na 2.4GHz rozhraní s prednastaveným unikátnym ESSID v tvare `UPC1234567` a vygenerovaným heslom. Toto heslo je veľmi slabé z pohľadu komplexnosti aj z pohľadu náhodnosti. Heslo je dlhé 8 znakov a obsahuje len veľké písmená (komplexita 26^8 ≈ 2^38) čo znamená, že rozbitie zachyteného hashu je otázka rádovo hodín až dní. Chyba v pseudonáhodnosti generovania hesla má za dôsledok, že heslo sa dá dopočítať na základe znalosti ESSID a BSSID [5].

Nedokumentované správcovské rozhranie

Router mal prístupné nedokumentované správcovske rozhranie na CLI (angl. command line interface) prostredníctvom nešifrovaného protokolu Telnet. Prihlasovacie údaje správcu boli `admin:admin`, pričom tieto boli nezávislé od používateľa webrozhrania. To znamená, že zmena hesla jedného používateľa nemenila heslo druhého používateľa. Bol k dispozícii aj ďalší používateľ `root:pega#123`. V oboch prípadoch sa jednalo o prístup superpoužívateľa (UID 0) cez `/bin/sh` k celému súborovému systému zariadenia – t.j. aj k súborom a programom operačného systému a webovej aplikácie. *[zraniteľný firmvér v. 1.0.20, zraniteľnosť bola prítomná minimálne od septembra 2015]*
Správcovske webrozhranie je prístupné aj na staticky nakonfigurovanej IP adrese 192.168.100.1. *[zraniteľný firmvér v. 2.07b]*

Zraniteľnosti súvisiace s fyzickým prístupom k zariadeniu

Pre úplnosť uvádzame aj nami neoverené zraniteľnosti reportované v článku [7], ktoré popisujú zraniteľnosti vedúce k získaniu prístupu k správcovskému príkazovému riadku (shell). Medzi zraniteľnosti patrí: 1) je vyvedené sériové UART rozhranie poskytujúce heslom chránený prístup k shell-u, 2) pri pripájaní USB kľúča sa kontroloval názov kľúča a existencia súboru s názvom `.auto` a ak sa našiel, vykonal sa ako skript správcovského shellu. *[verzia firmvéru neuvedená, článok z 17.1.2016]*

Zraniteľnosti procesov operátora

Operátor spravuje firmvér zariadení prenajatých jeho zákazníkmi. Operátor podľa potreby aktualizuje firmvér na novšiu verziu a deje sa tak bez predošlého upozornenia zákazníka e-mailom alebo telefonicky. Aktualizácia v lete 2016 spôsobila, že nami predtým zmenené heslo telnet používateľa 'admin' bolo opäť vo východzom stave (t.j. 'admin'). Poukazuje to na nedokonalosti procesu tvorby aktualizácií a ich nasadzovania, ktoré môžu viesť k zavedeniu zraniteľností.

Operátor odporúča vykonať zmenu prednastaveného ESSID aj hesla. Okrem toho však neposkytuje zákazníkom dbajúcim na súkromie a bezpečnosť žiadny návod na hardenovanie nastavení prenajatých zariadení, ktorý by napríklad odporúčal zmeniť heslo na správcovské webrozhranie, vypnúť WPS a podobne. [6]

CSIRT.SK ako aj iné organizácie či analytici opakovane notifikovali operátora o prítomnosti zraniteľností spolu s ich opisom. Niektoré zraniteľnosti boli odstránené (napríklad správcovské rozhranie cez Telnet), no niektoré závažné zraniteľnosti pretrvávajú (napríklad slabé prednastavené prihlasovacie údaje na správcovské webrozhranie). Operátor nenotifikoval dotknutých používateľov o tom, že zariadenie je zraniteľné a aké kroky k náprave by mali zákazníci vykonať. Ukazuje to, že v procese odstraňovania ohlásených zraniteľností je priestor na zlepšenie. Taktiež chýba proces varovania zákazníkov o zraniteľnostiach a potenciálnych dopadoch.

Charakter niektorých nájdených zraniteľností poukazuje na to, že operátor pri zavádzaní nového zariadenia do svojho portfólia alebo pri zmene vo firmvéri nevykonáva ohodnotenia zabezpečenia a zraniteľností produktu v potrebnom rozsahu.

2.2. Príklady scenárov útokov na siete s Ubee EVW3226

Pre ilustráciu možnosti zneužitia opísaných zraniteľností uvádzame opis niekoľkých scenárov jednoduchých útokov.

Scenár 1

Útočník vo fyzickej blízkosti (čo môže byť aj stovky metrov) preskenuje bezdrôtové médium a určí, či sa v blízkosti nachádza sieť s názvom (ESSID) vo východzom tvare. Zachytí aj príslušnú adresu prístupového bodu (BSSID) a využitím nástroja implementujúceho dopočítanie hesla určí heslo siete. Ak heslo nebolo menené, útočník sa pripojí a má prístup k lokálnej sieti obete a cez ňu prístup k sieti Internet. Celková náročnosť tohto útoku je veľmi nízka.

[6] Takýto návod sme si žiadali telefonicky prostredníctvom podpory používateľa.

Scenár 2

Útočník, ktorý už má prístup do siete, sa prostredníctvom protokolu Telnet pripojí na smerovač a autentifikuje sa využitím známych prihlasovacích údajov. Následne môže využiť niektoré štandardné linuxové nástroje ako napríklad `tcpdump` na odpočúvanie komunikácie prechádzajúcej smerovačom.

Útočník môže za určitých okolností aj modifikovať komunikáciu prechádzajúcu smerovačom. Jedná sa však už o pokročilý útok, nakoľko je nutné na smerovač dodať ďalšie programy implementujúce potrebnú funkcionalitu.

Scenár 3

Útočník, ktorý už má prístup do siete, môže zneužiť jednu z opísaných zraniteľností správcovského webrozhrania k získaniu prístupu naň (napríklad zadné dvierka alebo jednoduché východzie prihlasovacie údaje alebo slovníkový útok na autentifikáciu).

Následne môže napríklad zmeniť adresy používaných DNS serverov na servery ovládané útočníkom. Takto je možné presmerovať komunikáciu pre vybrané doménové mená na útočníkom zvolené IP adresy, pričom útok sa dotkne všetkých zariadní v LAN, ktoré si DNS servery nastavujú na základe DHCP.

Útočník môže taktiež nastaviť port-forwarding / PAT z WAN rozhrania na LAN – t.j. sprístupniť niektoré služby v internej sieti priamo zo siete operátora. V prípade, že router má verejnú IP adresu, znamená to sprístupnenie danej služby z Internetu. Následne môže útočník pristupovať alebo útočiť na dané služby v LAN priamo z Internetu.

2.3. Časový priebeh analýzy a nahlásenia zraniteľností

CSIRT.SK kontaktoval UPC Slovakia s upozornením na prítomnosť zraniteľností a dostupnosť exploitov opakovane od 27.7.2016.

- jún-júl 2016 – analytici CSIRT.SK sa oboznámili s publikovanou prácou iných analytikov o zraniteľnostiach EVW3226, overili prítomnosť zraniteľností a identifikovali ďalšie zraniteľnosti.
- 27.7.2016 – CSIRT.SK kontaktoval UPC Slovakia s upozornením na publikované zraniteľnosti aj na zraniteľnosti identifikované analytikmi CSIRT.SK so žiadosťou o poskytnutie odporúčaní zákazníkom adresujúce nájdené zraniteľnosti a poskytnutie informácie o plánovanom čase nasadenia aktualizácie firmvéru.
- 28.7.2016 – 11.8.2016 mailová a telefonická komunikácia s UPC Slovakia.
- Júl-august – zdieľanie informácii o zraniteľnostiach s GovCERT-hungary a informovanie konštituencie CSIRT.SK.
- 12.8.2016 – zverejnenie varovania na stránke www.csirt.gov.sk a informovanie konštituencie CSIRT.SK.
- Medzi augustom 2016 – februárom 2017 – časť zraniteľností bola odstránená tichou aktualizáciou firmvéru.

Z komunikácie s UPC Slovakia vyplynulo, že Ubee EVW3226 je starý model a zákazníci majú možnosť vymeniť si ho za niektorý aktuálne poskytovaný model. Zraniteľnosť prednastaveného hesla na „wifi“ bola adresovaná tým, že spoločnosť od začiatku poskytovania „wifi“ modemov odporúča klientom ako prvé vykonať zmenu prednastaveného mena a hesla pre „wifi“. Súčasťou bola informácia o tom, že pripravujú nový firmvér, ktorý bude klientov upozorňovať na potrebu zmeny hesla.

Naša žiadosť o poskytnutie oficiálneho stanoviska k ostatným zraniteľnostiam nebola zodpovedaná.

Časová os analýzy zraniteľností a komunikácie s operátorom a výrobcom zariadení je k dispozícii v článkoch jednotlivých analytikov.

2.4. Možnosti zmiernenia rizík

Nápravu väčšiny zraniteľností môže zabezpečiť len operátor, nakoľko zariadenie je v jeho správe.

Ak sa zákazník nechce spoliehať na udržiavanie požadovanej úrovne zabezpečenia firmvéru takéhoto zariadenia, tak ako čiastočné riešenie tejto situácie sa ponúka možnosť, že zákazník si zakúpi a nakonfiguruje vlastné zariadenie prostredníctvom ktorého sa pripojí k sieti operátora. K tomuto je však nutným predpokladom, že operátor vôbec povolí použitie vlastného zariadenia a taktiež poskytne zákazníkovi potrebnú technickú špecifikáciu a konfiguračné parametre[7]. Alternatívne je samozrejme možné za zraniteľné zariadenie umiestniť vlastný smerovač, ktorý bude spravovať lokálnu sieť, a za ktorého bezpečnosť bude zodpovedný výhradne zákazník.

3. Zhodnotenie

Opísali sme niekoľko zraniteľností domáceho smerovača rozšíreného v mnohých slovenských domácnostiach. Na základe testov [3] a našich skúseností konštatujeme, že obdobným typom zraniteľností trpia aj mnohé iné zariadenia používané v domácich LAN. Myslíme si, že je to dané najmä tým, že 1) pri tvorbe firmvéru sa v dostatočnej miere nedbá na bezpečnosť návrhu a produktu, 2) a tým, že operátori pri zavádzaní nového zariadenia do svojho portfólia alebo pri zmene vo firmvéri nevykonávajú ohodnotenia zabezpečenia a zraniteľností produktu v potrebnom rozsahu.

Cieľom tohto príspevku bolo poukázať na to, že aj jednoúčelné krabičky – domáce smerovače – môžu obsahovať viaceré závažné a miestami, žiaľ, aj triviálne zneužiteľné zraniteľnosti. Cieľom príspevku bolo taktiež upozorniť, že k našej domácej sieti sa tak nejak automaticky staviame ako k sieti, v ktorej máme svoje súkromie a zariadenia do nej pripojené sú v bezpečí – avšak ako sme poukázali v tomto článku, nemusí tomu tak byť. Chceme zdôrazniť, že zneužitie zraniteľností domáceho smerovača môže mať závažný dopad na súkromie, majetok a dobré meno používateľa. Mali by sme mať na pamäti, že aj našu domácu sieť je potrebné hardenovať taktiež ako všetky zariadenia, ktoré sú do nej pripájané. Špeciálne v prípade pripájania pracovných zariadení do domácej siete je potrebné, aby sa tieto zariadenia k sieti správali ako k akejkoľvek verejnej sieti a pre potreby pripojenia do pracovnej siete využívali technológiu VPN.

Referencie

[1] Oficiálna dokumentácia k smerovaču Ubee EVW3226 od spoločnosti UPC BROADBAND SLOVAKIA s.r.o.: https://www.upc.sk/content/dam/www-upc-sk/_docs/navod_ubee.pdf, navštívené 28.2.2017.

[2] Článok „Wardriving Bratislava 10/2016“ od yolosec.team: https://deadcode.me/blog/2016/11/05/Wardriving-Bratislava-10-2016.html, navštívené 28.2.2017.

[7] Podľa vyjadrenia zákazníckej podpory UPC možnosť použitia vlastného iného zariadenia nepodporuje. Dotazovali sme sa telefonicky dvakrát - v máji 2015 a v auguste 2016.

[3] Článok „Analysis of WiFi-enabled ISP modems“ od SEARCH-LAB Ltd: http://www.search-lab.hu/advisories/secadv-20150720, navštívené 28.2.2017.
[4] Security Advisory o zraniteľnostiach Ubee EVW3226 od SEC Consult Vulnerability Lab: https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20160602_Ubee_EVW3226_Multiple_critical_vulnerabilities_v10.txt, navštívené 28.2.2017.
[5] Článok „UPC UBEE EVW3226 WPA2 Password Reverse Engineering, rev 3“ od yolosec.team: https://deadcode.me/blog/2016/11/05/Wardriving-Bratislava-10-2016.html, navštívené 28.2.2017.
[6] CSIRT.SK: Varovanie pre používateľov WiFi smerovača Ubee EVW3226: https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=148, navštívené 28.2.2017.
[7] Článok „UPC Ubee EVW3226 Fail“ of Firefart: https://firefart.at/post/upc_ubee_fail/, navštívené 28.2.2017.