**Tisková zpráva** **JON.CZ, 27.8.2014**

# Backdoor do routerů Netis? Ne!

JON.CZ[1] je výhradním distributorem WiFi routerů a dalších síťových prvků Netis v Čechách a na Slovensku. Routery Netis[2] dodávané na náš trh jsou vyvíjeny zejména s ohledem na potřeby poskytovatelů internetového připojení (ISP). Disponují řadou funkcí (hardware NAT, podpora VLAN, provoz IPTV, funkce bridge, přístup pomocí Telnet z LAN, autokonfigurační soubor a další), které nejsou dostupné u výrobků jiných značek, zaměřených na trh domácností a malých firem. Tažným koněm těchto routerů jsou osvědčené RISC32 síťové procesory Realtek. Bezpečnost těchto zařízení je prvořadým cílem vedle jejich výkonu a poměru cena/výkon. JON.CZ je také významným poskytovatelem připojení k internetu ve středočeském regionu, který ve vlastní síti nasadil a používá téměř 5.000 kusů routerů Netis různých typů. Více než 50.000 routerů Netis slouží v sítích jiných ISP v ČR.

Některé české weby přinesly zprávu, že routery Netis obsahují chybu v zabezpečení "zadní vrátka", neboli "backdoor". Mezi prvními byl root.cz[3], který uvádí i zdroj této zprávy, tedy blog.trendmicro.com[4]. Originální zpráva, na kterou přímo nebo nepřímo odkazují všechny zprávy, je dostupná zde. Jde o první a jedinou zprávu od tohoto autora, nikdy předtím na tomto serveru nepublikoval.

JON.CZ otestoval routery Netis, které dodává na náš trh, konkrétně modely WF2411, WF2415, WF2501, WF2419 a WF2780 se všemi dostupnými verzemi firmware. Žádný z těchto routerů není možné napadnout způsobem uvedeným v článku, a to ani na uvedeném portu UDP 53413, ani na žádném jiném UDP portu od 1 do 65535. Detaily jsou uvedeny v technické části zprávy dále v dokumentu.

JON.CZ je připraven na vyžádání poskytnout routery Netis k nezávislým testům zájemcům z řad novinářů, odborné i široké veřejnosti.

**Jan Jirka, JON.CZ**
jan.jirka@jon.cz
www.netis.cz

---------- konec tiskové zprávy ----------
---------- následuje technický rozbor ----------

[1] http://www.jon.cz
[2] http://www.netis.cz
[3] http://www.root.cz/zpravicky/routery-netis-obsahuji-zadni-vratka/
[4] http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/

# Technický rozbor

## *Identifikace "backdooru"*

Originální zpráva, na kterou se odkazují zprávy odvozené je zde: http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/.

Autor ve své zprávě uvádí, že nalezl jakýsi “otevřený” UDP port 53413 na WAN rozhraní routeru. Údajně zjistil, že na portu žije služba XDMCP. Přitom z výpisu testu je patrné, že nalezl daný port ve stavu ***"open|filtered"***. Autor neuvádí, o který typ routeru mělo jít, přesto že je snadné tuto informaci zjistit z rozhraní routeru. Vedle dalších údajů uvádí výpis programu netstat z testovacího počítače, kde prezentuje uskutečněné spojení na cílový UDP port 53413.

## *Zjištěný stav*

1) **nmap** [5] prohlásí za "***open|filtered***" [6] všechny UDP porty, na které nedostane po dotazu odpověď, například pokud je paket zahozen firewallem. (více zde: ). Ve skutečnosti nmap prohlásí za ***"open|filtered”*** kterýkoliv port UDP od 1 do 65535, tedy včetně zmiňovaného portu 53413, protože nedostane od routeru žádnou odpověď. To však neznamená, že je router dostupný na daném portu, nýbrž pravý opak.

2) Služba **XDMCP**[7] je "X Display Manager Control Protocol”, podobně jako RDP nebo VNC jde o službu umožňující vzdálený přístup do grafického sytému X (např. Xfree86). Žádný takový grafický systém nikdy nebyl a s ohledem na velikost vnitřní paměti routerů ani nemohl být nikdy v routerech Netis instalován.

3) Výpis programu **netstat**[8] uvádí aktivní spojení na port UDP 53413. Tento výpis je pořízen na testovacím počítači, nikoliv na routeru. Protože UDP je nespojovaný (connectionless) protokol, stačí otevřít daný port ze zdrojového počítače a bez ohledu na to, zda je spojení skutečně funkční, bude uvedeno ve výpisu netstat jako uskutečněné/spojené. Tento údaj je naprosto nevypovídající.

---

[5] http://nmap.org
[6] http://nmap.org/book/man-port-scanning-basics.html
[7] http://www.faqs.org/docs/Linux-HOWTO/XDMCP-HOWTO.html
[8] http://www.faqs.org/docs/linux_network/x-087-2-iface.netstat.html

## *Důkaz*

**1) Test otevřených portů.**
Proveďte příkaz "***nmap -T4 -sU -p 53413 -v 192.168.3.1***", kde volbou ***-p*** určíte UDP port (můžete zadat i rozsah, například "1-100" nebo "1-65535") a poslední údaj nahradíte IP adresou WAN rozhraní routeru.

Odpověď bude zhruba tato:

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-27 01:36 CEST
Initiating ARP Ping Scan at 01:36
Scanning 192.168.3.1 [1 port]
Completed ARP Ping Scan at 01:36, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:36
Completed Parallel DNS resolution of 1 host. at 01:36, 0.02s elapsed
Initiating UDP Scan at 01:36
Scanning 192.168.3.1 [1 port]
Completed UDP Scan at 01:36, 0.23s elapsed (1 total ports)
Nmap scan report for 10.0.0.1
Host is up (0.00048s latency).
PORT      STATE         SERVICE
53413/udp open|filtered unknown
MAC Address: 08:10:77:85:06:6C (Unknown)
```

**2) Otevření UDP spojení.**
Proveďte příkaz ***"nc -vu 192.168.3.1 53413"*** a ponechte program otevřený (ukončíte později příkazem ***"q"***). Program se pokusí vytvořit spojení a dokonce sdělí, že spojení úspěšně vytvořil:

```
found 0 associations
found 1 connections:
     1:      flags=82<CONNECTED,PREFERRED>
       outif (null)
       src 192.168.10.49 port 64753
       dst 192.168.3.1 port 53413
       rank info not available

Connection to 192.168.3.1 port 53413 [udp/*] succeeded!
```

Nejde však o spojení pomocí protokolu TCP, takže program pouze oznamuje, že je připraven vysílat data na tento UDP port a případně přijmout odpovědi. Neví nic o tom, že cílová strana data nepřijme.

**3) Výpis netstat.**
Nyní proveďte příkaz ***"netstat -a -p UDP"***, který vypíše spojení uskutečněná protokolem UDP. Výpis je zkrácen:

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
udp4       0      0  192.168.10.49.55288    1-3-168-192.j.53413
```

Výpis programu netstat "potvrzuje", že probíhá spojení na daný UDP port. Protože však nepoužíváme protokol spojovaný (TCP), je tato informace značně neurčitá. Ve skutečnosti je v cíli veškerý provoz zahazován (drop), ale protokol UDP o tom z principu nemůže vědět.

## *Závěr*

Autor originálního článku si zřejmě mylně vysvětlil význam stavu "open|filtered" v programu **nmap**. Ve skutečnosti není možné uvedený UDP port na WAN rozhraní otevřít na žádném z testovaných zařízení. Jako další důkaz uvádí výpis z programu **netstat**, který však žádným důkazem není a z principu funkce protokolu UDP ani důkazem být nemůže.

Díky důkladné znalosti a praktickým zkušenostem s routery Netis si dovoluji tvrdit, že v žádném z uvedených routerů není od výrobce uvedeno žádné přihlašovací jméno nebo heslo. Bohužel nelze přinést důkaz o neexistenci něčeho, co prostě není.

Zajímavé je, že přestože autor tvrdí, že se mu podařilo popisovaný průnik uskutečnit, neuvádí, o jaký typ routeru šlo. Ve skutečnosti by to snadno zjistil, pokud by se dovnitř dostal. Místo toho tvrdí, že téměř všechny routery Netis/Netcore mají tuto slabinu ("Almost all Netcore/Netis routers appear to have this vulnerability"). Toto tvrzení je vyvráceno našimi testy. Podle mne není pravděpodobné, že existuje routeru Netis, do kterého by bylo možné takto proniknout, rozhodně však nejde o žádný router z výše jmenovaných.

---------- konec technického rozboru ----------