noho z honeypotů sdružení CSIRT.CZ. Následně byli jeho členové dotčeným ISP informováni o napadeném zařízení CPE, které ve své síti právě testoval, a na základě spolupráce s dodavatelem pak mohli učinit níže popsané kroky.

Prvotní analýza

Nejprve ze všeho je třeba zdokumentovat stav zařízení – tj. před připojením do internetové sítě. Především je třeba se seznámit se zařízením a určit jeho základní chování v bezpečném prostředí. Zaprvé se tím dá vyhnout případné nové infekci a zadruhé se v případě trvalého nakažení vyhneme rozšíření nákazy po internetu.

Trvale nakažené routery jsou v dnešní době přinejmenším neobvyklé, zanedbat je ale nelze. Ve chvíli, kdyby se testované zařízení například snažilo hned po startu skenovat náhodné IP adresy v internetu, je to celkem jasná indicie, že k takovému nakažení došlo.

Pro začátek je dobré zjistit především dostupnost síťových portů jak na rozhraní pro lokální síť, tak směrem do internetu. Dále je třeba co možná nejpřesněji identifikovat jednotlivé služby. Zvláště pak ty, které jsou dostupné z vnějšku.

Běžný router by neměl mít z vnějšku dostupné prakticky vůbec nic. Některé modely mají přístupné například webové rozhraní pro vzdálenou zprávu, ale doporučuje se ji vypnout vzhledem k velkému počtu zranitelností v poslední době.

U analyzovaného zařízení Billion BiPAC 9800VNXL byly z vnější sítě dostupné porty 5555 a 7547. Jak již bylo uvedeno, tyto porty jsou určeny pro ISP pro vzdálenou správu a uživatel obvykle nemá možnost je zablokovat.

Pro získání a ověření detailních informací je třeba, aby mělo zařízení dostupný (ideálně linuxový) shell například přes ssh nebo alespoň telnet.

Bohužel v tomto případě tomu tak nebylo. Funkcionalita příkazové řádky byla velmi omezená a jediný užitečný příkaz byl k zobrazení verze firmwaru.

```
telnet 192.168.1.254
admin>sys version
1.11.rc14
```

[Trvale nakažené routery jsou v dnešní době přinejmenším neobvyklé, zanedbat je ale nelze.]

[Router byl připojen k internetu ani ne dvě hodiny, když přijal příchozí spojení na portu 7547 a rázem začal stahovat soubor ze vzdáleného TFTP serveru.]

Analýza komunikace

Další částí analýzy je chování zařízení v síti. K tomu se výborně hodí nástroj Wireshark – k prozkoumání chování routeru na lokální síti a potom na vnějším rozhraní po připojení do internetu. Mezi běžnou komunikaci po připojení do internetu patří například synchronizace času přes NTP a kontrola aktualizací.

Nicméně samovolně odchozí komunikaci je dobré prověřovat a alespoň se pokusit určit, proč a kam daná komunikace směřuje. Ještě zajímavější je pak příchozí komunikace, která není odmítnutá.

Router byl připojen k internetu ani ne dvě hodiny, když přijal příchozí spojení na portu 7547 a rázem začal stahovat soubor ze vzdáleného TFTP serveru.

Po rychlém odpojení zařízení od internetu a následném zkoumání komunikace vyšlo najevo, že došlo ke zneužití pro tento model dosud nezdokumentované zranitelnosti. A poté se spustil následující příkaz, který způsobil stažení malwaru a jeho spuštění.

Po vzoru moderních botnetů (jako například Hajime) malware nejprve zablokoval příchozí spojení na zranitelných portech, aby ho jiný malware později nenahradil, a následně začal komunikovat s ostatními stroji v botnetu a snažil se najít další zranitelná zařízení, ale hned se ručně odpojil.

Druhotná analýza

S využitím nových znalostí se mohla dokončit celková analýza firmwaru zkoumaného zařízení. Po zjištění běžících procesů a dostupných programů v zařízení pomocí příkazů poslaných přes využitou zranitelnost se vypnul běžící telnet pomocí *killall utelnetd* a následně zapnul s jinými parametry *utelnetd -l /bin/sh -d*.

Nyní již nic nebránilo vyextrahování celého firmwaru, který byl uložen v oddílech *mtd0-4*. Následným porovnáním firmwaru z analyzovaného zařízení a čistého firmwaru pomocí utility sha256sum se prokázalo, že nákaza nezanechala trvalé následky.

Nahlášení zranitelnosti

Protože šlo o nezdokumentovanou zranitelnost a nová aktualizace firmwaru nebyla dostupná, kontaktoval se výrobce s nahlášením této zranitelnosti. Kromě toho je třeba zranitelnost nahlásit do databáze zranitelností CVE, kterou provozuje společnost Mitre.

Ta na základě dostupných informací vyhodnotí vážnost zranitelnosti vyjádřenou číslem CVSS a přiřadí jí unikátní CVE-ID.

Shodou okolností se podobná a popsaná zranitelnost vyskytuje i na modemu Eir D1000 (a pravděpodobně i na mnohých dalších) a do té doby ještě nebyla v databázi zavedená. Po konzultaci s Mitre došlo k zavedení nového CVE-2016-10372 a zranitelnost se označila jako kritická.

Co dál?

Zhruba takto může dopadnout jednoduché hlášení z honeypotu.

Nutno dodat, že aktualizace firmwaru již existuje, ale bohužel pro dodavatele nebyla na zapůjčeném routeru ani dostupná ke stažení z internetu. ■

Autor pracuje jako bezpečnostní analytik sdružení CZ.NIC.