MikroTikPatch Biztonsági Elemzés (részletes)

Dátum: 2025-06-01

Tesztkörnyezet: A vizsgálat egy virtuális gépen (x86 architektúra) futtatott MikroTik RouterOS 7.19.1 patchelt verzióján történt. A hozzáférést a WebFig felületen keresztül, valamint SSH kapcsolaton keresztül végeztük. A rendszer a belső hálózaton működött, teszt célból korlátozott külső kapcsolatokat is lehetővé téve (pl. SSH kimenet). Az elemzés célja a nyilvános forráskódú patchelt rendszer biztonsági szempontú átvilágítása volt.

Vizsgálat végezte: ChatGPT (József)

1. Fájlstruktúra-elemzés

A rendszer kulcskönyvtárai átvizsgálásra kerültek: /flash, /rw, /etc, /home, /var. A patchelt image fájlok jellemzően a jogosultságellenőrzés kikapcsolását célozzák, külön binárisok vagy nem dokumentált szkriptek nem kerültek elő. A változtatások főként az /rw könyvtárban, valamint a startup mechanizmusban találhatók.

2. Rendszerindítás és időzített szkriptek

A /system script és /system scheduler kimenetek alapján a rendszerindítás során nem futnak ismeretlen vagy rejtett időzített szkriptek. A gyári indítási folyamat egészében megtartott, a patchelt rendszer csak az engedélyellenőrzést módosítja.

3. Rendszerlog és hálózati forgalom

A logkövetés (/log print follow) és csomagfigyelés (/tool sniffer) alapján a rendszer nem indít kimenő kapcsolatokat ismeretlen címekre. Nem figyelhető meg DNS-lekérdezés, HTTP- vagy HTTPS-hívás a rendszer részéről. A WebFig és SSH kapcsolatok manuális használata során sem történt automatikus adatátvitel harmadik fél felé.

4. Biztonsági beállítások és szolgáltatások

Az alapértelmezett szolgáltatások (SSH, Winbox, API, WebFig) aktívak és jelszóval védettek. Tűzfalon jelenleg nincs külön korlátozás. A jelszavak nem olvashatók vissza a felületről. Javasolt az IP-szűrés és port-hozzáférések szabályozása zárt környezeten kívüli használat esetén.

5. Külső SSH-kapcsolat teszt

Egy külső szerverre történő SSH-kapcsolatot sikeresen létesítettünk a routerről. A kapcsolat stabil maradt, nem volt szakadás vagy újracsatlakozás szükséges. A hálózati interfészek viselkedése stabil, a NAT és routing működése megbízhatónak tűnik tesztkörnyezetben.

6. Összegzés és következtetés

A MikroTikPatch projekt által kínált módosított RouterOS image technikailag stabilnak és tisztának tűnik a vizsgált 7.19.1-es verzió alapján. Nem észleltünk sem rejtett hálózati aktivitást, sem hátsó ajtót. A rendszer ajánlott zárt, fejlesztési vagy tesztkörnyezetben való használatra. Éles, nyilvános hálózaton történő használat esetén fokozott körültekintés javasolt.

Forrásmegjelölés és megosztás

Ez a dokumentum az OpenAI ChatGPT (József) által készített biztonsági elemzés a MikroTikPatch projekt 7.19.1 verziójához. A vizsgálat a https://github.com/elseif/MikroTikPatch forráskód és az ott elérhető image-fájl alapján készült. A rendszer ideiglenes hozzáférését és a tesztelési környezetet Skori (skori.pwm.hu) biztosította. A dokumentum szabadon megosztható változtatás nélkül, a forrás feltüntetésével.