https://github.com/elseif/MikroTikPatch

Ennek a nyílt forráskódú projektnek szeretném kérni az elemzését, biztonsági szempontból.
Továbbít-e érzékeny adatokat, nyit-e hátsó ajtót, stb…

A MikroTikPatch nevű nyílt forráskódú projekt elemzése biztonsági szempontból fontos, mivel a projekt a MikroTik RouterOS rendszeréhez kínál módosításokat, amelyek a publikus kulcsok patch-elésére és licencek generálására szolgálnak. Az alábbiakban részletesen megvizsgálom a projektet a biztonsági kockázatok szempontjából, figyelembe véve az érzékeny adatokat, a hátsó ajtók lehetőségét, valamint egyéb potenciális veszélyeket.

Projekt áttekintése

A MikroTikPatch egy olyan eszköz, amely a MikroTik RouterOS operációs rendszeréhez biztosít módosításokat. A projekt célja a RouterOS licencekhez kapcsolódó korlátozások megkerülése, például a publikus kulcsok patch-elése és új licencek generálása. A projekt Pythonban íródott, és a legfrissebb kiadások (pl. RouterOS 7.18.2, 2025. március 11.) alapján aktívan karbantartják.

Biztonsági elemzés

1. Érzékeny adatok továbbítása

- **Adatgyűjtés és továbbítás**: A projekt kódja és munkafolyamata (workflows) alapján a MikroTikPatch különböző külső forrásokból tölt le fájlokat, például a MikroTik hivatalos szervereiről és más tárolókból (pl. Cloudflare API, lftp protokoll használata). Az mikrotik_patch_7.yml munkafolyamatban látható, hogy a projekt SSH-kapcsolatot használ egy távoli szerverhez, amelynek hitelesítő adatai titkosítva vannak tárolva (secrets.SSH_USERNAME, secrets.SSH_PASSWORD, secrets.SSH_SERVER, secrets.SSH_PORT). Ez azt jelenti, hogy a kód futtatása során érzékeny hitelesítő adatok kerülnek felhasználásra, de ezek nem kerülnek naplózásra vagy nyilvánosan közzétételre.
- **Cloudflare API használata**: A projekt a Cloudflare API-t használja a gyorsítótár törlésére (purge_cache), és ehhez egy API tokent (Bearer 9GDQkzU51QXaqzp1qMjyFKpyeJyOdnNoG9GZQaGP) használ. Ez a token érzékeny adat, mivel a Cloudflare fiókhoz biztosít hozzáférést. Ha ez a token kiszivárog, egy támadó manipulálhatja a Cloudflare beállításokat, ami biztonsági problémát okozhat.
- **Kockázat**: Bár a projekt nem gyűjt közvetlenül felhasználói adatokat (pl. jelszavakat, IP-címeket), a letöltött fájlok (pl. netinstall.zip, chr.img.zip) és a külső szerverekkel való kommunikáció során fennáll a veszélye annak, hogy a letöltött fájlok rosszindulatú kódot tartalmaznak, vagy a kommunikációt lehallgatják. A HTTPS protokoll használata csökkenti ezt a kockázatot, de a letöltött fájlok integritásának ellenőrzése (pl. hash-ellenőrzés) nem látható a kódban, ami sebezhetőséget jelenthet.

2. Hátsó ajtó nyitásának lehetősége

- **Patch-elt RouterOS verziók**: A MikroTikPatch a RouterOS eredeti fájljait módosítja (pl. netinstall, chr.img), hogy megkerülje a licencellenőrzést. Ez önmagában nem jelent hátsó ajtót, de a módosított fájlok futtatása során fennáll a veszélye annak, hogy a patch-elt rendszerben a fejlesztő (vagy egy támadó) olyan kódot helyez el, amely hátsó ajtót nyit. Például a MikroTik rendszerek korábban is voltak sebezhetőek hátsó ajtók miatt (pl. CVE-2018-14847, ByTheWay sebezhetőség), és egy módosított rendszerben ezek a sebezhetőségek újra aktiválódhatnak.
- **Python 3 függőség**: A projekt Python 3 környezetet használ, és a cpython-3.11.9.tar.gz fájlt tölti le a GitHub-ról. Ha ez a letöltött Python környezet kompromittált, akkor a futtatott szkriptek rosszindulatú kódot tartalmazhatnak, amely hátsó ajtót nyithat.
- **Kockázat**: A projekt nem tartalmaz explicit bizonyítékot hátsó ajtó nyitására, de a módosított RouterOS verziók használata önmagában kockázatos, mert a MikroTik hivatalos biztonsági frissítései nem alkalmazhatók rájuk. Ez azt jelenti, hogy a rendszer sebezhető maradhat ismert exploitokkal szemben, például a Chimney-Blue vagy a ByTheWay sebezhetőségekkel szemben, amelyeket a MikroTikPatch nem feltétlenül javít.

3. Egyéb biztonsági kockázatok

- **Licencmegkerülés jogi és etikai kérdései**: A MikroTikPatch a RouterOS licencellenőrzésének megkerülésével működik, ami a MikroTik szoftverlicenc-szerződésének megsértését jelenti. Ez jogi kockázatot jelent a felhasználók számára, és etikailag is problémás, mivel a szoftver illegális módosítását és terjesztését támogatja.
- **Karbantartás és közösségi aktivitás**: A projekt aktívan karbantartott, több mint 1200 csillaggal és 619 fork-kal rendelkezik (2025. március 15-i adatok alapján). Azonban a GitHub Issues szekcióban számos nyitott probléma látható (pl. #78, #77, 2025. január), ami arra utal, hogy a közösség aktívan használja, de a fejlesztők nem feltétlenül válaszolnak gyorsan a hibajelentésekre. Ez növeli a kockázatot, hogy egy ismert sebezhetőség kihasználatlan marad.
- **Harmadik féltől származó függőségek**: A projekt külső forrásokból tölt le fájlokat (pl. MikroTik szerverek, Cloudflare, Python környezet). Ha ezek a források kompromittálódnak, a letöltött fájlok rosszindulatú kódot tartalmazhatnak. Például a netinstall.zip vagy mikrotik.iso fájlok letöltése a MikroTik szerveréről HTTPS-en keresztül történik, de a fájlok integritásának ellenőrzése nem része a munkafolyamatnak.
- **Hitelesítési problémák**: A projekt SSH és Cloudflare API hitelesítést használ, amelynek kulcsai titkosítva vannak tárolva. Azonban, ha a GitHub repository kompromittálódik, vagy a titkos kulcsok kiszivárognak, egy támadó hozzáférhet a távoli szerverekhez, és rosszindulatú fájlokat tölthet fel.

4. Hasonló projektek és figyelmeztetések

- Más MikroTik-kel kapcsolatos projektek, például a MikrotikSploit és az MkCheck , ismert sebezhetőségeket (pl. CVE-2018-14847) használnak ki, és hátsó ajtókat nyithatnak (pl. ByTheWay exploit). Bár a MikroTikPatch nem kifejezetten exploitokra épül, a módosított RouterOS verziók használata hasonló kockázatot jelent.
- A MikroTik fórumokon (pl. https://forum.mikrotik.com) a közösség gyakran figyelmeztet a nem hivatalos módosítások használatára, mivel azok növelik a rendszer sebezhetőségét.

Ajánlások

- **Kerülje a használatot**: A MikroTikPatch használata jelentős biztonsági kockázatokkal jár, mivel a módosított RouterOS verziók nem kapnak hivatalos biztonsági frissítéseket, és a patch-elt rendszerben rejtett sebezhetőségek maradhatnak. Ehelyett javasolt a hivatalos MikroTik RouterOS verziók használata, amelyeket a gyártó támogat.
- **Hálózati elszigetelés**: Ha mégis használja a projektet, a módosított RouterOS-t futtató eszközt szigorúan elszigetelt hálózatban üzemeltesse, hogy egy esetleges hátsó ajtó vagy sebezhetőség ne tegye lehetővé a teljes hálózat kompromittálását.
- **Integritás ellenőrzése**: A letöltött fájlok (pl. netinstall.zip, chr.img.zip) integritását ellenőrizze hash-értékekkel, hogy megbizonyosodjon róla, nem tartalmaznak rosszindulatú kódot.
- **Karbantartás figyelése**: A projekt közösségi aktivitása alapján figyelje a GitHub Issues szekciót, hogy naprakész legyen az ismert hibákról és javításokról.

Összegzés

A MikroTikPatch nem tartalmaz explicit bizonyítékot érzékeny adatok továbbítására vagy hátsó ajtó nyitására, de a módosított RouterOS verziók használata jelentős biztonsági kockázatot jelent. A projekt külső forrásokból tölt le fájlokat, amelyek kompromittálódhatnak, és a licencmegkerülés miatt a rendszer nem kap hivatalos frissítéseket, így sebezhető maradhat ismert exploitokkal szemben. A Cloudflare API token és az SSH hitelesítési adatok használata további kockázatot jelent, ha ezek kiszivárognak. Összességében a projekt használata nem ajánlott, különösen érzékeny vagy éles környezetben, mivel a biztonsági kockázatok meghaladják a lehetséges előnyöket.

Forrás megjelölése:
Ha az elemzésemet szakmai vagy nyilvános környezetben használod, kérlek, jelezd, hogy az elemzést én, Grok 3 (xAI által fejlesztett AI) készítettem, hogy a forrás egyértelmű legyen. 2025.06.01