TLP:CLEAR
Szabadon terjeszthető!

Riasztás az Axios npm csomag kompromittálódásról

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** (NBSZ NKI) riasztást ad ki az **Axios JavaScript könyvtár npm ellátási láncát érintő kritikus kompromittálódás miatt**. A rendelkezésre álló információk szerint 2026. március 31-én a támadók kompromittálták az Axios npm csomag egyes verzióit, amelyek mindössze körülbelül **három órán keresztül voltak elérhetők**, azonban ez az időablak is elegendő volt ahhoz, hogy **automatikus CI/CD folyamatok, fejlesztői munkaállomások, valamint akár éles (production) környezetek is emberi beavatkozás nélkül telepítsék azokat**.

A kompromittált Axios csomagok egy rosszindulatú *plain-crypto-js@4.2.1* függőséget tartalmaztak. A legitim Axios csomag a megszokott függőségeken túl **nem használ ilyen komponenst**, ezért a **plain-crypto-js megjelenése anomáliának tekinthető**. A támadók a beszámolók szerint egyetlen új függőség hozzáadásával érték el, hogy a fertőzött csomag telepítésekor a rosszindulatú kód lefusson, majd a rendszerből érzékeny adatokat gyűjtsön, és platformfüggő **hátsó kaput** (backdoor) **telepítsen**.

A támadási lánc során a támadók először egy *plain-crypto-js@4.2.0* csomagot publikáltak, majd ezt követően megjelent a rosszindulatú *plain-crypto-js@4.2.1 verzió*. Ezt követően jelent meg az *axios@0.30.4, majd az axios@1.14.1,* így **rövid időn belül mindkét fő verzióág érintetté vált**. A rendelkezésre álló információk szerint a **dropper obfuszkált formában működött**, fordított Base64 kódolást, valamint egy „OrDeR_7077” kulccsal végrehajtott XOR műveletet alkalmazva.

Amennyiben az npm list Axios parancs eredménye 1.14.1 vagy 0.30.4 verziót mutat, az adott rendszert potenciálisan kompromittáltnak kell tekinteni. Ilyen esetben erősen javasolt az **érintett rendszer teljes újratelepítése**, valamint az összes ott használt hitelesítő adat, token és kulcs haladéktalan cseréje.

Az érintett verziók a rendelkezésre álló információk szerint a következők:

- *axios@1.14.1*
- *axios@0.30.4*

A javasolt biztonságos verziók:

- *axios@1.14.0 és az összes korábbi 1.x verzió*
- *axios@0.30.3 és az összes korábbi 0.x verzió*

Fontos kiemelni, hogy bár kizárólag a 1.14.1 és 0.30.4 verziók bizonyultak rosszindulatúak, **a régebbi kiadások ettől függetlenül tartalmazhatnak egyéb ismert biztonsági hibákat**, ezért a legcélszerűbb visszaállási pont az axios@1.14.0, illetve a axios@0.30.3. Emellett **javasolt a verziók rögzítése is**, mivel a caret (^) jelölés automatikus patch frissítést engedhet, ami ellátási lánc támadás esetén további kockázatot jelenthet.

A kompromittációhoz kapcsolódó **ismert hálózati indikátorok közé tartoznak** az alábbiak:

- *sfrclak[.]com,*
- *callnrwise[.]com,*
- *142[.]11.206.73,*
- *8000*/tcp port.

Emellett gyanús forgalomként kezelendők a

- *packages[.]npm.org/product0,*
- *packages[.]npm.org/product1,*
- *packages[.]npm.org/product2*

útvonalakra irányuló POST kérések is.

Az ismert, kapcsolódó e-mail indikátorok:

- *ifstap@proton[.]me*
- *nrwise@proton[.]me*

Az ismert csomag- és fájlhash-ek az alábbiak:

- axios@1.14.1 SHA-1: *2553649f2322049666871cea80a5d0d6adc700ca*
- axios@1.14.1 MD5: *21d2470cae072cf2d027d473d168158c*
- axios@1.14.1 SHA-256: *5bb67e88846096f1f8d42a0f0350c9c46260591567612ff9af46f98d1b7571cd*
- axios@0.30.4 SHA-1: *d6f3f62fd3b9f5432f5782b62d8cfd5247d5ee71*
- axios@0.30.4 SHA-256: *59336a964f110c25c112bcc5adca7090296b54ab33fa95c0744b94f8a0d80c0f*
- plain-crypto-js@4.2.1 SHA-1: *07d889e2dadce6f3910dcbc253317d28ca61c766*
- plain-crypto-js@4.2.1 MD5: *db7f4c82c732e8b107492cae419740ab*
- plain-crypto-js@4.2.1 SHA-256: *58401c195fe0a6204b42f5f90995ece5fab74ce7c69c67a24c61a057325af668*
- setup.js MD5: *7658962ae060a222c0058cd4e979bfa1*
- setup.js SHA-1: *b0e0f12f1be57dc67fa375e860cedd19553c464d*
- setup.js SHA-256: *e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09*
- system.bat MD5: *089e2872016f75a5223b5e02c184dfec*
- system.bat SHA-1: *978407431d75885228e0776913543992a9eb7cc4*
- system.bat SHA-256: *f7d335205b8d7b20208fb3ef93ee6dc817905dc3ae0c10a0b164f4e7d07121cd*
- Windows második fázisú 6202033 PowerShell RAT MD5: *04e3073b3cd5c5bfcde6f575ecf6e8c1*
- Windows második fázisú 6202033 PowerShell RAT SHA-1: *a90c26e7cbb3440ac1cad75cf351cbedef7744a8*
- Windows második fázisú 6202033 PowerShell RAT SHA-256: *617b67a8e1210e4fc87c92d1d1da45a2f311c08d26e89b12307cf583c900d101*
- macOS payload (com.apple.act.mond) MD5: *7a9ddef00f69477b96252ca234fcbeeb*
- macOS payload (com.apple.act.mond) SHA-1: *13ab317c5dcab9af2d1bdb22118b9f09f8a4038e*
- macOS payload (com.apple.act.mond) SHA-256: *92ff08773995ebc8d55ec4b8e1a225d0d1e51efa4ef88b8849d0071230c9645a*

- Linux payload (ld.py) MD5: *9663665850cdd8fe12e30a671e5c4e6f*
- Linux payload (ld.py) SHA-1: *59faac136680104948e083b3b67a70af9bfa5d5e*
- Linux payload (ld.py) SHA-256: *fcb81618bb15edfdedfb638b4c08a2af9cac9ecfa551af135a8402bf980375cf*
- Windows perzisztenciafájl (system.bat) MD5: *8c782b59a786f18520673e8d669e3b0a*
- Windows perzisztenciafájl (system.bat) SHA-1: *ae39c4c550ad656622736134035f17ca7a66a742*
- Windows perzisztenciafájl (system.bat) SHA-256: *e49c2732fb9861548208a78e72996b9c3c470b6b562576924bcc3a9fb75bf9ff.*

A platformfüggő ismert kompromittációs nyomok közé tartoznak:

- macOS alatt: /Library/Caches/com.apple.act.mond
- Linux alatt: /tmp/ld.py
- Windows alatt: C:\ProgramData\wt.exe, C:\ProgramData\system.bat, valamint %TEMP%\6202033.vbs és %TEMP%\6202033.ps1

Ezek jelenléte kompromittációra utalhat, ugyanakkor hiányuk önmagában nem zárja ki a fertőzést, mivel a rosszindulatú kód megkísérelheti a nyomainak eltávolítását.

Javasolt intézkedések

- Amennyiben az érintett rendszerben az *axios@1.14.1* vagy *axios@0.30.4* verzió előfordul, a gépet kompromittáltnak kell tekinteni.
- Javasolt az érintett csomag azonnali eltávolítása és az *axios@1.14.0*, illetve *axios@0.30.3* verzióra történő visszaállás.
- Javasolt a *package-lock.json*, *yarn.lock* és egyéb lockfile-ok, valamint a Git-előzmények ellenőrzése a *plain-crypto-js* előfordulására.
- Javasolt az ismert kompromittációs nyomok keresése a fájlrendszeren, valamint az aktív vagy korábbi C2 kommunikáció vizsgálata.
- Javasolt az összes npm token, SSH kulcs, felhős hozzáférési kulcs, API token és egyéb hitelesítő adat azonnali visszavonása és cseréje.
- Javasolt az érintett rendszerek teljes újraépítése, mivel a puszta törlés vagy csomagcsere nem tekinthető elegendő helyreállítási intézkedésnek.
- Hosszabb távon javasolt a pontos verziórögzítés, az npm ci használata, a lifecycle scriptek korlátozása, valamint a frissen publikált csomagverziók késleltetett elfogadása.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833