TLP:WHITE
Szabadon terjeszthető!

Rendkívüli tájékoztatás
ICS/SCADA rendszerek elleni támadások kapcsán

(2022. április 14.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **tájékoztatást** ad ki a **US-CERT** által közzétett, fejlett fenyegetési (APT) csoportokhoz köthető, ipari vezérlőrendszerek (ICS) és felügyeleti vezérlő- és adatgyűjtő (SCADA) eszközök elleni kibertámadások kapcsán. A támadók egyedi eszközöket fejlesztettek ki az ICS/SCADA eszközök keresésére, kompromittálására, és a hozzáférés megszerzésére, ezenkívül egy, az **ASRock alaplap-illesztőprogramjában** lévő ismert sérülékenységen keresztül feltörhetik a Windows-alapú munkaállomásokat. Az ICS/SCADA eszközök kompromittálásával és emelt szintű hozzáférés megszerzésével a támadók megzavarhatják az eszközök tevékenységét, vagy egyes funkcióikat.

Érintett eszközök:

- Schneider Electric MODICON és MODICON Nano PLC-k, ideértve ─ de nem kizárólagosan ─ a TM251, TM241, M258, M238, LMC058, és LMC078 modelleket.
- OMRON Sysmac NJ és NX PLC, ideértve ─ de nem kizárólagosan ─ a NEX NX1P2, NX-SL3300, NX-ECC203, NJ501-1300, S8VK, és R88D-1SN10F-ECT modelleket.
- OPC Unified Architecture (OPC UA) szerverek.

A támadásokhoz használt moduláris felépítésű eszközök segítségével automatizált támadások is végrehajthatóak.

Javaslatok:

- Az ICS/SCADA rendszerek különválasztása a vállalati és internetes hálózatoktól, a köztes kommunikáció korlátozása.
- Többlépcsős hitelesítés (MFA) alkalmazása az ICS rendszerekhez és eszközökhöz minden egyes távoli hozzáférés esetén.
- Incidenskezelési terv készítése, és rendszeres gyakorlatok tartása.
- A jelszavak kötelező, periodikus cseréje, az alapértelmezett jelszavak megváltoztatása.
- Rendszeres offline mentés készítése.
- Az ICS/SCADA rendszerek hálózati kapcsolatainak korlátozása.
- Végpontvédelmi (EDR) eszközök alkalmazása.
- Folyamatos OT rendszermonitoring.
- Csak a legszükségesebb alkalmazások telepítése.
- Legkisebb jogosultság elvének alkalmazása.
- A rendszerek folyamatos monitorozása a szokatlan illesztőprogramok ─ mint például az ASRock, amennyiben az alapértelemezetten nincs használatban ─ betöltődésének megakadályozásához.

TLP:WHITE
Szabadon terjeszthető!

Hivatkozások:

- https://www.cisa.gov/uscert/ncas/alerts/aa22-103a
- https://thehackernews.com/2022/04/us-warns-of-apt-hackers-targeting.html
- https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu