14. Hírlevél az ipari irányító rendszerek biztonságáról

A Black Cell elkötelezett az ipari irányító rendszerek (Industrial Control Systems – ICS), és/vagy kritikus infrastruktúrák biztonságának megteremtésében, ezért havonta hírlevelet bocsát ki a témában. A hírlevélben az érintett szervezetek, illetve kritikus infrastruktúra üzemeltetők tájékozódhatnak, valamint információkat nyerhetnek az ipari irányító rendszerek sérülékenységeiről; jó gyakorlatokról; a témát érintő képzésekről, oktatásokról, és konferenciákról; az ipari irányító rendszerek üzemeltetőit ért incidensekről. Az ipari irányító rendszerek biztonságáról szóló könyveket is ajánlunk, lehetőség szerint online elérhetőséggel. A Black Cell javaslatokat, megoldásokat kínál az ipari irányító rendszerekhez kapcsolódó tevékenységek hatékony elvégzéséhez, és ezáltal a biztonság minél magasabb szintű megteremtéséhez. A hírlevélben foglaltakkal kapcsolatosan bővebb információért forduljon bizalommal a cara (kukac) blackcell.hu e-mail címen szakértőinkhez.

Tartalom:

ICS jó gyakorlatok, javaslatok

Az industrialcyber.co kiadott egy info grafikát, amellyel az ICS rendszereket üzemeltető szervezeteknek kívánnak segítséget nyújtani a megfelelő szintű biztonság megteremtéséhez.

Az info grafika tartalmaz egy 10-es listát, amely a napi ICS folyamatok védelmét szolgálja. Az ICS üzemeltetőknek javasolt a listában szereplő ajánlásokat átvizsgálni, és a tapasztalt hiányosságokat megszűntetni. A 10-es lista a következő ajánlásokból áll:

1. Priorizáld, ellenőrizd, teszteld és telepítsd az ICS rendszerekhez kiadott javító csomagokat (patch-eket)!
2. Mentsd a rendszer konfigurációt, és a rendszer adatokat!
3. Azonosítsd, minimalizáld és tedd biztonságossá az ICS kapcsolatokat!
4. Folyamatosan ellenőrizze és értékelje az ICS hálózatok kapcsolatainak biztonságát!
5. Tiltsa le a nem szükséges szolgáltatásokat, portokat és protokollokat!
6. Használja a rendelkezésre álló biztonsági beállításokat, konfigurációs megoldásokat!
7. Alkalmazzon alkalmazás fehér listát (whitelisting) és antivírus megoldást!
8. Az üzemeltetők és az adminisztrátorok részére szervezzen ICS biztonsági oktatást!
9. Tartsa karban és folyamatosan tesztelje az incidenskezelési eljárásrendet!
10. Alakítson ki kockázat alapú mélységi védelmi megoldást hálózat és kliens szinten egyaránt!

A tudatosító anyag a holnap kihívásait is górcső alá veszi, és a következő témában fogalmaz meg ajánlásokat a jövőt illetően:

- Kockázatmenedzsment és kiberbiztonsági szabályozás,
- Fizikai biztonság,
- ICS hálózati architektúra,
- ICS hálózat és periméter biztonság,
- Host biztonság,
- A biztonság monitorozása,
- Ellátási lánc menedzsment,
- Humán elem.

A dokumentum tartalmazza a 2019-es év legelterjedtebb kockázatait és gyengeségeit a határvédelem, a legkisebb funkcionalitás alapelvei, az azonosítás és hitelesítés, fizikai és logikai hozzáférés tekintetében.

Az info grafika a következő linken érhető el:

https://industrialcyber.co/wp-content/uploads/2020/05/2020.05.26-Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

ICS képzések, oktatások

A teljeség igénye nélkül 2020. júliusban, ICS biztonság tárgyában a SANS nem tart ICS képzéseket, oktatásokat, a COVID-19 világjárványra tekintettel, kizárólag online formában.

A részletek a következő webhelyen találhatók:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Időszakosan induló online kurzusok:

A https://www.coursera.org/ honlapon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során video oktatásokon vehet részt a jelentkező, és feladatok megoldásával demonstrálhatja tudását a szakterületet érintően. Az online tanfolyam elvégzését követően a Univesity of Colorado Boulder tanúsítványt állít ki a végzettek részére. A következő kurzusok végezhetők el:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

További részletek a következő webhelyen találhatók:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

Az említett oktatásokon felül az ICS-CERT is kínál Online kurzusokat:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity
- ICS Evaluation

További részletek a következő webhelyen találhatók:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

Az **ICS-CERT Virtual Learning Portal** (VLP) a következő képzések elvégzését teszi lehetővé:

- Operational Security (OPSEC) for Control Systems (100W) - 1 óra
- Differences in Deployments of ICS (210W-1) – 1.5 óra
- Influence of Common IT Components on ICS (210W-2) – 1.5 óra
- Common ICS Components (210W-3) – 1.5 óra
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 óra
- Cybersecurity Risk (210W-5) – 1.5 óra
- Current Trends (Threat) (210W-6) – 1.5 óra
- Current Trends (Vulnerabilities) (210W-7) – 1.5 óra
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 óra

- Attack Methodologies in IT & ICS (210W-9) – 1.5 óra
- Mapping IT Defense-in-Depth Security Solutions to ICS (210W-10) – 1.5 óra

A részletek a VLP képzések ugyanazon a linken érhetők el, mint a többi ICS-CERT online kurzus.

A SANS online képzései az ipari irányító rendszerek biztonságával kapcsolatban:

- ICS410: ICS/SCADA Security Essentials

További részletek a következő webhelyen találhatók:

https://www.sans.org/find-training-beta/search?courses=2762&types=10&redirect=beta#__utma=195150004.1547647064.1563952209.1566466056.1568274011.4&__utmb=195150004.2.9.1568274014545&__utmc=195150004&__utmx=-&__utmz=195150004.1568274011.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=17428089

Az ipari irányító rendszerek és a SCADA rendszerek biztonságáról szóló Online kurzus érhető el az Udemy honlapján, ahol a jelentkező megtanulhatja az ICS/SCADA biztonság alapjait, technológiai megoldásokat, szoftver kezelést, szabályozási megoldásokat.

- ICS/SCADA Cyber Security

További részletek a következő webhelyen találhatók:

https://www.udemy.com/ics-scada-cyber-security/

A Department of Homeland Security 2 napos képzése során a résztvevők megismerhetik a különböző vezérlő rendszerek biztonságával kapcsolatos tudnivalókat.

- SCADA security training

A koronavírus világjárványra tekintettel az online kurzusok élő közvetítéssel valósulnak meg.

További részletek a következő webhelyen találhatók:

https://www.tonex.com/training-courses/scada-security-training/

A SCADAhacker-com honlapon is megtalálható az ipari irányító rendszerek biztonságáról szóló online kurzus:

- Understanding, Assessing and Securing Industrial Control Systems

Az oktatás 40-120 órát vesz igénybe, és 8 modul segít eligazodni az ICS rendszerek kiberbiztonságának világában. A képzés a „blue teaming” tevékenységre fókuszál az ICS és SCADA rendszerek vonatkozásában.

A képzés alkalmas bizonyos képesítéssel rendelkező személyek (például: CISSP, CEH stb.) tudásának ICS specifikusság tételére.

További részletek a következő webhelyen találhatók:

https://scadahacker.com/training.html

A School of security ICS és SCADA Rendszerek biztonsági oktatást tart online, mely oktatás felkészíti a résztvevőket, hogy tanúsított SCADA biztonsági szakemberek legyenek (Certified SCADA Security Architect).

Az oktatás az ICS és SCADA rendszerek alapjait, sérülékenységeit, kockázatmenedzsment alapjait, biztonsági kontrollok implementációit, szerver biztonságát, hálózat- és eszköz biztonságát, biztonsági programjainak fejlesztését, és a hálózat nélküli SCADA biztonságot mutatja be részletesen.

A tanfolyamok 0-3 vagy 4-12 hónap időtávban van lehetőség elvégezni, igény szerint. A részletekkel kapcsolatos további információ a következő honlapon található:

https://www.enosecurity.com/training-tutorials-courses/ics-scada-security-essentials-training/

Az INFOSEC-Flex SCADA/ICS Security Training Boot Camp elnevezésű online oktatása lehetőséget biztonsít a SCADA és ICS rendszerek elleni külső és belső támadások elleni felkészülésre.

A kurzus elvégzése garanciát ad a réztvevőknek arra, hogy tanúsított SCADA biztonsági szakemberek legyenek (Certified SCADA Security Architect).

A 4 napos online kurzus leghamarabbi időpontja, melyre lehet regisztrálni a következő:

2020. 08. 03 – 07. Ezt követően a következő kurzus 2020. szeptemberben kerül megrendezésre.

A SCADA és ICS biztonsági alapjain kívül a szabályozási környezet is részleteiben bemutatásra kerül, ahogy a SCADA biztonsági kontrollok, és a SCADA penteszt is.

A képzéssel kapcsolatos további információk a következő linken érhetők el:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

ICS konferenciák

2020. júliusában a koronavírus járványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop vagy elmarad, vagy valamely későbbi időpontra került eltolásra. Az alábbi konferenciák azonban virtuálisan kerülnek megtartásra.

ICS Lockdown

A SecurityWeek ICS kiberbiztonsági konferenciáján a résztvevők megismerkedhetnek a Microsoft IT/OT kiberbiztonsági kultúrával, új OT biuztonsági playbook-kal, és számos más ipari kiberbiztonsággal kapcsolatos újdonsággal egyaránt.

ICS Lockdown; (SecurityWeek – virtuális), 2020. július 8-9.

További információk a következő linken találhatók:

https://www.securitysummits.com/event/ics-lockdown/

ICS incidensek

A Honda üzemeltetési és IT rendszereit Ransomware támadás érte

A Honda autógyártási rendszerében szervereket ért Ekans malware támadás, amely a gyártás leállását okozta. A 2020. június 8-án történt támadást a korai órákban észlelte a szervezet kiberbiztonsági szoftvere. A virustotal.com weboldalon is publikálásra került a káros kód.

A támadás nem csak az IT rendszert, hanem az OT rendszert is érintette, a termelési, értékesítési és fejlesztési tevékenységek folytonossága is sérült. A Honda tájékoztatása szerint a szervezet egész hálózatában elterjedt a malware.

A vállalat megerősítette, hogy az Egyesült Királyságban működő üzem legállt, az Észak-Amerikában, Törökországban, Olaszországban és Japánban folytatott egyéb feladatok felfüggesztése mellett végzik a szervezetek tevékenységeiket.

Az Ekans vagy Snake ransomware kifejezetten az ipari irányító rendszerekre specializálódott. A Honda tájékoztatása szerint a kezelt adatok nem kompromittálódtak, és az üzleti hatása a támadásnak minimális.

A kibervédelmi szakemberek és a szervezet szakemberei egyaránt a globális pandémia helyzetet tekintik annak a kiváltó körülménynek, amely miatt a támadók COVID-19 témájú káros tartalommal ellátott e-mailekkel támadták áldozataikat, akik ilyen helyzetben fogékonyak a megosztásra, és a „jótékony célú kattintásra”, hogy segítséget nyújthassanak.

A Honda a tavalyi évben is szenvedett el kibertámadást, akkor az ElasticSearch adatbázisból került ki 40 GigaBájtnyi adat, amely a szervezet rendszereiről és munkavállalóról tartalmazott érzékeny adatokat.

Szerző: Bár jelenleg számszerűsített adat (pénzösszeg) nincs arra vonatkozólag, hogy mekkora kárt okoztak a támadók, kizárólag annyit tudunk, hogy minimális hatást publikált a Honda az esemény következményeként. Ilyen nemzetközi szervezet esetében azonban ez jelenthet dollármilliókat is, amely valószínűsíthetően az információbiztonság tudatosság hiányára vezethető vissza, ha az incidenssel kapcsolatban megjelent információknak hinni lehet. Javasoljuk, hogy a világ politikai-, és emberek milliárdjait érdeklő egyéb események (COVID-19 járvány) megjelenése esetén a tudatosító kampányok foglalkozzanak az ezzel kapcsolatos „Social Engineering” támadások lehetőségeivel, ezzel csökkentve a humán tényező miatti kockázatokat.

Az incidenssel kapcsolatos további információk a következő webhelyeken érhetők el:

https://www.computing.co.uk/news/4016242/honda-suffers-suspected-ransomware-attack

https://www.telegraph.co.uk/business/2020/06/08/honda-could-victim-ransomware-cyber-attack/

https://www.bbc.com/news/technology-52982427

Könyvajánló

Az ipari irányító rendszerek és a SCADA kiberbiztonsági kutatásainak harmadik nemzetközi szimpóziuma a témában jártas kutatók fóruma. A kutatók számos érdekes kutatási eredményt osztottak meg a témát illetően a kiadás évében, 2015-ben.

A könyv tartalmazza a hardver, továbbá az emberi tényezők szempontjából lefolytatott kutatási eredményeket. Az ICS kiberbiztonsági kérdéseinek széles spektrumát lefedi a könyv tartalma, az automatizált eszköz azonosításon át a behatolás észlelésén keresztül az aktív védelemig, továbbá a behatolás detektációra használt honeypot-okig.

Az ICS és SCADA rendszereket ért incidensekre adandó válaszok, illetve a forensic vizsgálatok is részét képezik a szimpóziumról kiadott könyvnek.

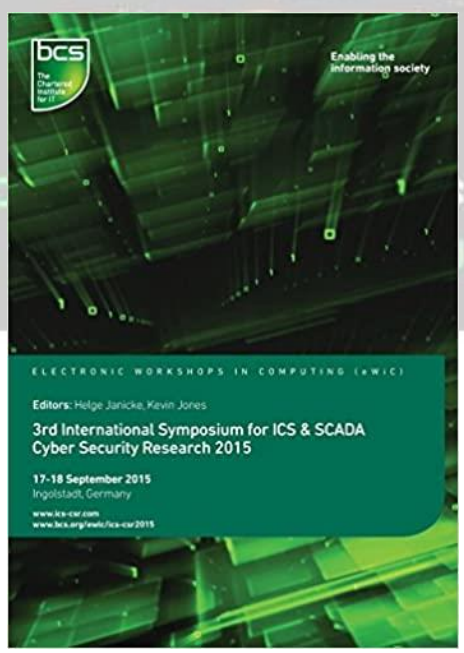
A könyv címe: Third International Symposium for ICS & SCADA Cyber Security

Szerzők/szerkesztők: Helge Janicke, Kevin Jones.

Kiadás éve: 2015.

A kiadvány elérhető a következő linken:

https://www.amazon.co.uk/dp/1780173172?slotNum=14&linkCode=g12&imprToken=QsdXk5pEbWBqHuAVgdWBow&creativeASIN=1780173172&tag=uuid07-21



Black Cell javaslatok

Egy Siemens által publikált jelentés szerint az OT elleni támadások 30%-ban detektálanul maradnak. Ez hatalmas probléma, mivel nem lehet biztos egy ipari irányító rendszert üzemeltető szervezet abban, hogy biztonságosan működik.

Annak érdekében, hogy az OT működésében tisztában legyen a szervezet a fenyegetésekkel, meg kell értenie azt, hogy milyen fenyegetések leselkednek a rendszereire. A MITRE ATT&CK for ICS Matrix táblázat bemutatja azokat a taktikákat, technikákat, amelyek veszélyt jelenthetnek az ipari rendszerekre, és amelyekkel a támadók dolgozhatnak.

A táblázat segítséget nyújt abban, hogy a fenyegetettségi térképet megismerve fel tudjuk készíteni a rendszereinket arra, hogy a bizonyos fajta támadásokat milyen módon észleljenek, milyen technikát, vagy milyen technológiát kell alkalmazni annak érdekében, hogy a bevezető részben említett 30% lecsökkenhessen 5% alá.

Ha a szervezet OT biztonsági szakértői tisztában vannak a lehetséges fenyegetésekkel, az implementálandó intézkedések kiválasztása már csupán kockázatelemzés, üzleti hatáselemzés, költség-haszon elemzés, és beszerzési eljárás lefolytatásának a függvénye.

Számos szervezet elköveti azt a hibát, hogy IPS, IDS, vagy SIEM rendszereket szereznek be anélkül, hogy pontosan tudnák, mire van szükségük. A felső vezetés megnyugszik, hogy drága forintokért (dollárokért) bevezet egy rendszert, anélkül, hogy lenne szakértelem annak üzemeltetésére, használatára, vagy a meglévő infrastruktúra azt támogatná. Egy ilyen rendszer bevezetése előtt fel kell mérni minden olyan tényt, amely gondot okozhat.

A MITRE ATT&CK for ICS oldalon számos további hasznos információ található a táblázat mellett, például az ICS elleni támadások technikáinak teljes listája, annak a 17 szoftvernek a listája, amelyet a MITRE ATT&CK követ, az ICS incidensek mögött álló APT csoportok listája és jellemzése, vagy az ICS rendszerekben használt eszközök jellemzése.

Javasolt a teljes dokumentum áttanulmányozása annak érdekében, hogy a teljes ICS biztonságot fenyegető környezetet megértse egy szervezet, és mint tudásbázist használja a szervezet ICS biztonsági stratégiájának és védelmének kialakítása során.

ICS sérülékenységek

2020. júniusában az alábbi ipari irányító rendszereket érintő sérülékenységeket publikálta a National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs), vagyis az ICS-CERT:

ICSMA-20-177-01: **Philips Ultrasound Systems**
Alacsony szintű sérülékenység: hitelesítés alternatív csatornán vagy úton történő megkerülése.
https://www.us-cert.gov/ics/advisories/icsma-20-177-01

ICSA-20-177-01: **ENTTEC Lighting Controllers**
Magas szintű sérülékenységek: beégetett kriptográfiai kulcs használata, XSS, nem megfelelő hozzáférés ellenőrzés, kritikus erőforráshoz történő helytelen hozzáférés hozzárendelés.
https://www.us-cert.gov/ics/advisories/icsa-20-177-01

ICSA-20-177-02: **Rockwell FactoryTalk Services Platform XXE**
Magas szintű sérülékenység: nem megfelelő XML korlátozás.
https://www.us-cert.gov/ics/advisories/icsa-20-177-02

ICSA-20-177-03: **Rockwell FactoryTalk View SE**
Magas szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő továbbítása, gyenge jelszó kódolás.
https://www.us-cert.gov/ics/advisories/icsa-20-177-03

ICSA-20-175-01: **Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L and FX Series CPU Modules**
Kritikus szintű sérülékenység: érzékeny információk egyszerű szöveges formában történő továbbítása.
https://www.us-cert.gov/ics/advisories/icsa-20-175-01

ICSA-20-175-02: **Honeywell ControlEdge PLC and RTU**
Közepes szintű sérülékenység: érzékeny információk egyszerű szöveges formában történő továbbítása.
https://www.us-cert.gov/ics/advisories/icsa-20-175-02

ICSA-20-175-03: **ABB Device Library Wizard**
Magas szintű sérülékenység: érzékeny információk nem biztonságos tárolása.
https://www.us-cert.gov/ics/advisories/icsa-20-175-03

ICSMA-20-170-01: **Baxter ExactaMix**
Magas szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő továbbítása, beégetett jelszó használat, érzékeny információk hiányzó titkosítása, nem megfelelő hozzáférés ellenőrzés, erőforrás kitettség, nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsma-20-170-01

ICSMA-20-170-02: **Baxter PrismaFlex and PrisMax**
Magas szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő továbbítása, nem megfelelő hitelesítés, beégetett jelszó használat.

https://www.us-cert.gov/ics/advisories/icsma-20-170-02

ICSMA-20-170-03: **Baxter Phoenix Hemodialysis Delivery System**

Magas szintű sérülékenység: érzékeny információk egyszerű szöveges formában történő továbbítása.
https://www.us-cert.gov/ics/advisories/icsma-20-170-03

ICSMA-20-170-04: **Baxter Sigma Spectrum Infusion Pumps**

Magas szintű sérülékenységek: beégetett jelszó használata, érzékeny információk egyszerű szöveges formában történő továbbítása, kritikus erőforráshoz helytelen engedély hozzárendelés, műveleti probléma.
https://www.us-cert.gov/ics/advisories/icsma-20-170-04

ICSMA-20-170-05: **BIOTRONIK CardioMessenger II**

Alacsony szintű sérülékenységek: nem megfelelő hitelesítés, érzékeny információk egyszerű szöveges formában történő továbbítása, érzékeny adatok hiányzó titkosítása, jelszavak visszafejthető formában történő tárolása.
https://www.us-cert.gov/ics/advisories/icsma-20-170-05

ICSMA-20-170-06: **BD Alaris PCU**

Közepes szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsma-20-170-06

ICSA-20-170-01: **Johnson Controls exacqVision**

Közepes szintű sérülékenység: kriptográfiai aláírás hibás ellenőrzése.
https://www.us-cert.gov/ics/advisories/icsa-20-170-01

ICSA-20-170-02: **Mitsubishi Electric MC Works64, MC Works32**

Kritikus szintű sérülékenységek: memória határon kívüli írás lehetősége, alkalmazás adatkezelési problémák, kód befecskendezés.
https://www.us-cert.gov/ics/advisories/icsa-20-170-02

ICSA-20-170-03: **ICONICS GENESIS64, GENESIS32**

Kritikus szintű sérülékenységek: memória határon kívüli írás lehetősége, alkalmazás adatkezelési problémák, kód befecskendezés.
https://www.us-cert.gov/ics/advisories/icsa-20-170-03

ICSA-20-170-04: **Rockwell Automation FactoryTalk Services Platform**

Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-170-04

ICSA-20-170-05: **Rockwell Automation FactoryTalk View SE**

Kritikus szintű sérülékenységek: nem megfelelő bemeneti hitelesítés, műveletek memóriapuffer határain belüli nem megfelelő korlátozása, engedély, jogosultság és hozzáférés-vezérlő problémák, érzékeny információk feltárása.
https://www.us-cert.gov/ics/advisories/icsa-20-170-05

ICSA-20-168-01: Treck TCP/IP Stack (Update A)

Kritikus szintű sérülékenységek: a hosszparaméterek nem megfelelő kezelése, nem megfelelő bemeneti hitelesítés, memória címhívási probléma, memória puffer határain kívüli olvasás lehetősége, nem megfelelő hozzáférés ellenőrzés, egész szám túlcsordulás, nulla szám kezelési hiba.
https://www.us-cert.gov/ics/advisories/icsa-20-168-01

ICSA-20-161-02: Mitsubishi Electric MELSEC iQ-R series (Update A)

Közepes szintű sérülékenység: erőforrás kimerülés.
https://www.us-cert.gov/ics/advisories/icsa-20-161-02

ICSMA-20-163-01: Philips IntelliBridge Enterprise IBE

Alacsony szintű sérülékenység: Érzékeny információk naplófájlba történő beillesztése.
https://www.us-cert.gov/ics/advisories/icsma-20-163-01

ICSA-20-163-01: OSIsoft PI Web API 2019

Magas szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-20-163-01

ICSA-20-163-02: Rockwell Automation FactoryTalk Linx Software

Kritikus szintű sérülékenységek: nem megfelelő bementi hitelesítés, útvonal bejárás, veszélyes fájlfeltöltés korlátozásának hiánya.
https://www.us-cert.gov/ics/advisories/icsa-20-163-02

ICSA-20-161-01: Advantech WebAccess Node

Kritikus szintű sérülékenység: puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-20-161-01

ICSA-20-161-02: Mitsubishi Electric MELSEC iQ-R series

Közepes szintű sérülékenység: ellenőrizetlen erőforrás feltárás.
https://www.us-cert.gov/ics/advisories/icsa-20-161-02

ICSA-20-161-03: Siemens LOGO!

Kritikus szintű sérülékenység: kritikus funkció hiányzó hitelesítése.
https://www.us-cert.gov/ics/advisories/icsa-20-161-03

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK

Közepes szintű sérülékenységek: nem jegyzett keresési út vagy elem.
https://www.us-cert.gov/ics/advisories/icsa-20-161-04

ICSA-20-161-05: Siemens SIMATIC, SINAMICS

Magas szintű sérülékenységek: ellenőrizetlen elem a keresési útvonalban, puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-20-161-05

ICSA-20-161-06: Siemens SINUMERIK

Kritikus szintű sérülékenységek: kód átírás, puffer túlcsordulás, nem megfelelő inicializálás, határon kívüli olvasás lehetősége, a memóriahely elérése a puffer vége után, nem megfelelő érvénytelenítés.

https://www.us-cert.gov/ics/advisories/icsa-20-161-06

ICSA-20-133-02: OSIsoft PI System (Update A)

Magas szintű sérülékenységek: ellenőrizetlen elem a keresési útvonalban, kriptográfiai aláírás hibás ellenőrzése, helytelen alapértelmezett engedélyek, null pointer dereferencia, funkció kivétel hiba, nem megfelelő bemeneti hitelesítés, XSS, érzékeny információk beillesztése a naplófájlba.
https://www.us-cert.gov/ics/advisories/icsa-20-133-02

ICSA-19-253-03: Siemens Industrial Products (Update G)

Magas szintű sérülékenységek: túlzott adat lekérdezési műveletek, egész szám túlcsordulás, ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-253-03

ICSA-19-099-06: Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update H)

Magas szintű sérülékenység: memória puffer határain kívüli olvasás lehetősége.
https://www.us-cert.gov/ics/advisories/ICSA-19-099-06

ICSMA-18-228-01: Philips PageWriter TC10, TC20, TC30, TC50, and TC70 Cardiographs (Update A)

Közepes szintű sérülékenységek: nem megfelelő bemeneti hitelesítés, beégetett hitelesítők használata.
https://www.us-cert.gov/ics/advisories/ICSMA-18-228-01

ICSMA-19-080-01: Medtronic Conexus Radio Frequency Telemetry Protocol (Update B)

Kritikus szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, érzékeny információk egyszerű szöveges formában történő továbbítása.
https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

ICSA-20-154-01: ABB System 800xA

Magas szintű sérülékenység: helytelen alapértelmezett engedélyek.
https://www.us-cert.gov/ics/advisories/icsa-20-154-01

ICSA-20-154-02: ABB System 800xA Base

Magas szintű sérülékenység: helytelen engedély hozzárendelés a kritikus erőforráshoz.
https://www.us-cert.gov/ics/advisories/icsa-20-154-02

ICSA-20-154-03: ABB Multiple System 800xA Products

Magas szintű sérülékenység: helytelen alapértelmezett engedélyek.
https://www.us-cert.gov/ics/advisories/icsa-20-154-03

ICSA-20-154-04: ABB Central Licensing System

Kritikus szintű sérülékenységek: információ feltárás, XML külső entitás nem megfelelő korlátozása, ellenőrizetlen erőforrás felhasználás, engedélyek - jogosultságok és hozzáférés-vezérlők hibái, nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-154-04

ICSA-20-154-05: GE Grid Solutions Reason RT Clocks

Kritikus szintű sérülékenység: kritikus funkció hiányzó autentikációja.

https://www.us-cert.gov/ics/advisories/icsa-20-154-05

ICSA-20-154-06: SWARCO CPU LS4000

Kritikus szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-154-06

ICSA-20-147-01: Inductive Automation Ignition (Update A)

Kritikus szintű sérülékenységek: kritikus funkció hiányzó autentikációja, alkalmazás adatérvényesítési hiba.
https://www.us-cert.gov/ics/advisories/icsa-20-147-01

A sérülékenységek részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://ics-cert.us-cert.gov/advisories

A sérülékenységek részletes leírását, a megoldási javaslatokat, és az érintett termékek teljeskörű listáját a sérülékenységhez tartozó linken lehet megtalálni.

Javasolt a sérülékenységek folyamatos nyomon követése, mert a gyengeségek kezelésére és a sérülékenységek befoltozására vonatkozó releváns információk is megjelennek a részletes leírásokban.

ICS riasztások

2020. június hónapban az ICS-CERT nem adott ki riasztást.

A korábban kiadott riasztások részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://www.us-cert.gov/ics/alerts