19. 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 ENISA (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) október 20-án publikált számos 2020 évet érintő fenyegetettségi elemzést, amelyek a következő weboldalon megtalálhatók és onnan ingyenesen letölthetők:

https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

Megtalálható a különböző speciális fenyegetettségekre vonatkozó elemzés, mint például a ransomware, DDoS vagy a phishing támadások, de a web alapú támadásokról is közzétette az ENISA a fenyegetettségi térképét. Jelen hírlevében a szektorspecifikus elemzésről olvashat pár gondolatot az olvasó.

A kibertámadási trendek vonatkozásában a dokumentum bemutatja, hogy minden egyes szektorban nő a web alapú-, a phishing és a malware támadások száma. Azon szektorok, ahol ipari irányító rendszerek üzemeltetése tudható vagy feltételezhető, az egészségügyi szektorban nő a malware támadások, a belső fenyegetések (nem feltétlenül szándékos, de emberi hiba vagy támadás), és a web alapú támadások száma. Ugyanezen fenyegetések az infokommunikációs technológiák szektorban stagnálnak.

A gyártóipar sok esetben használ ICS/SCADA rendszereket, és ebben az ágazatban is stagnálnak az említett fenyegetések. Az elemzés szót ejt az 5G és az újgenerációs mobil kommunikáció komponenseinek-, az IoT (dolgok internete) és az okos kártyák (Smart cards) fenyegetettségi kitettségéről.

Az elemzésben megjegyzi a szerző, hogy a COVID-19 világjárvány miatti távoli munkavégzés következtében jelentősen megnőtt a phishing (adathalász) támadások száma, mert ez a helyzet megkönnyítette a támadók dolgát, az érzékeny információk könnyebben kiszivárogtak az elmúlt időszakban a szervezetektől.

A gyártási szektorban (ICS/SCADA üzemeltető szervezetek) az ellátási láncokat érintő támadások is megszaporodtak, amely rendkívül veszélyes, mert akár egy kritikus infrastruktúra teljes leállását is okozhatja az ellátási láncokat érintő kibertámadások következménye.

További információk a Sectoral/thematic threat analysis dokumentumban találhatók meg, mely a következő linken érhető el:

https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis

ICS képzések, oktatások

A COVID-19 világjárványra tekintettel 2020. decemberben ICS biztonság tárgyában a SANS kizárólag online formában tart ICS képzéseket, oktatásokat.

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/ weboldalon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során videóalapú oktatásokon vehet részt a jelentkező, és feladatok megoldásával demonstrálhatja tudását a szakterületet érintően. Az online tanfolyam elvégzését követően a University of Colorado Boulder tanúsítványt állít ki a tanfolyamot elvégző személyek részére. A következő kurzus végezhető el:

- 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
  - 2020.12.07-12.
  - 2020.12.14-19.

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, szoftverkezelést, 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 kétnapos képzése során a résztvevők megismerhetik a különböző vezérlőrendszerek 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

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

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

A 4 napos online kurzus a SCADA és ICS biztonsági alapjain kívül a szabályozási környezet is részleteiben bemutatja, ahogy a SCADA biztonsági kontrollokat és a SCADA penetrációs teszt is.

A képzéssel kapcsolatos további információk a következő linken érhetők el:

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

ICS konferenciák

2020. decemberében a koronavírus világjárványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop virtuálisan vagy a helyszínen biztonsági intézkedések betartása mellett kerül megtartásra.

WCICSS-2020

A konferencián az ipari irányító rendszerek biztonságával foglalkozó biztonsági szakemberek, menedzserek, szállítók, szolgáltatást nyújtók vesznek részt, akik fejlesztéssel, integrációval, értékeléssel, implementációval és üzemeltetéssel foglalkoznak. A konferencia a résztvevőknek lehetőséget biztosít a trendek, és a védelmi megoldások megvitatására a jelenlévő szakemberekkel.

A konferencia célja, hogy az akadémiai és az ipari szereplők közötti tudáskülönbségek eltűntetésre kerüljenek azáltal, hogy a releváns tudást az adott szakterületeket érintve megosztják egymással.

World Congress on Industrial Control Systems Security; (Virtuális konferencia, Egyesült Királyság, London); 2020.12.8-10.

További információk a következő linken találhatók:

https://wcicss.org/

ICS üzemeltetői incidensek

Kórházak elleni zsarolóvírus támadások

A brooklyni és a vermonti kórházak is áldozatul estek a Ryuk ransomware támadásnak 2020 októberében. Az Egyesült Államok figyelmeztetést adott ki az egészségügyi intézmények és szolgáltatók részére a fenyegetettségről.

A kibertámadást a UNC1878 nevű kelet európai hekker csoporthoz kötik, és kórházak százait támadják a zsarolóvírussal a Mandiant CTO-ja Charles Carmakal szerint. Az említett kórházak tekintetében megállapítható, hogy az egész szervezetre kiterjedő volt a zsarolóvírus támadás.

A brooklyni kórház bizonyos eszközök védelme érdekében a hálózatának bizonyos szegmenseit leválasztotta, de nem a megfelelő időben, így számos eszköz és az abban tárolt adatok is letitkosításra kerültek. A kórházi irányító rendszerek és az orvosi gyógyításhoz üzemeltetésbe állított eszközök működésképtelensége sok esetben emberéletekbe is kerülhet. Arról nincs nyilvános információ, hogy kellett-e emiatt betegeket más kórházakba átirányítani, vagy hogy milyen hatással volt a kibertámadás a betegek kezelésére.

A vermonti kórház nyilatkozata szerint volt hatása a kibertámadásnak és a betegrendelésben is történtek változások. A kórház biztosította a betegeket, hogy megfelelő eljárásrendek mentén biztosítja a kórház, hogy a megfelelő betegellátás működőképes maradhasson.

A fizetést a zsarolók részére nem javasolja semmilyen szervezet, főleg a Ryuk ransomware esetében, mert a dekódolás a fájlok megrongálódását eredményezheti.

Az Emsisoft felajánlotta az egészségügyi intézményeknek, hogy a pandémia időszaka alatt ingyenesen biztosítja a zsarolóvírusok dekódolásával kapcsolatos szolgáltatását.

A támadásokkal kapcsolatos bővebb információk a következő linken érhetők el:

https://www.bleepingcomputer.com/news/security/brooklyn-and-vermont-hospitals-are-latest-ryuk-ransomware-victims/

Szerző: Egy szervezetet sem etikus támadni, de ha lehet ilyet írni, az egészségügyi intézményeket még etikátlanabb. Az egyik legkiszolgáltatottabb ágazat az egészségügy, ahol az egészségügyi eszközök hálózatba kötve emberek életét biztosító adatokkal dolgoznak és sok esetben a kiberbiztonság másodrangú, mert az idő tényező miatt kevésbé állítanak be rétegzett logikai intézkedéseket ezen szervezetek. Ha a hazai viszonyokat nézzük, a technológiai biztonsághoz szükséges eszközpark is hiányos, vagy elavult, ezáltal még nehezebb a kibertámadások kivédése. Mindezek ellenére szükséges a kibervédelem, a biztonságtudatosság, és a szervezeti kockázatarányos védelem kialakítása, mert bizonyos ígéretek ellenére támadva vannak az egészségügyi szervezetek rendszerei, ahogy ebben az incidens leírásban is láthatjuk.

Könyvajánló

Az ipar 4.0 napjainkban sok szervezetet foglalkoztat. Azonban a biztonságos ipari irányító rendszerek megteremtése és üzemeltetése komplex, sok időt igénylő feladat. A Cybersecurity for Industry 4.0 című könyv segítséget nyújthat ennek kialakításában.

A könyvben kifejtésre kerül, hogy pontosan mi is az az ipar 4.0, valamint annak legfontosabb előnyei is bemutatásra kerülnek. A szerzők szót ejtenek a CAD titkosításokról, továbbá a kiberfizikai biztonság új megközelítéséről is. Tárgyalja a kiadvány a SCADA rendszerek Fonensic vizsgálatát az IIoT-n (ipari dolgok internete) belül, és a big data biztonságot az egészségügyi szektorban.

Az olvasó megismerkedhet a kiberbiztonsági kontrollok értékelésével és alkalmazásával, a következtetéseken alapuló behatolás érzékelő rendszerekkel. Mindenképp ajánlott olvasmány azon ipari irányító rendszert üzemeltető szervezeteknek, akik az ipar 4.0 alapulvételével szervezték vagy tervezik szervezni folyamataikat.

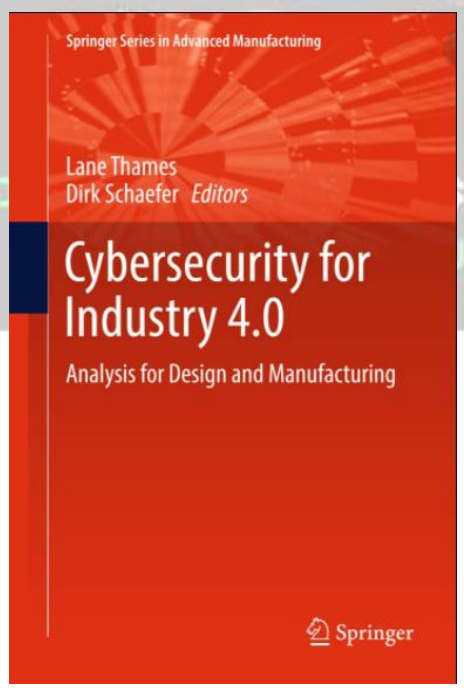
A könyv címe: Cybersecurity for Industry 4.0

Szerzők/szerkesztők: Lane Thames, Dirk Schaefer

Kiadás éve: 2017.

A kiadvány elérhető (és onnan letölthető) a következő linken:

https://link.springer.com/book/10.1007%2F978-3-319-50660-9



Black Cell javaslatok

Kiberbiztonsági kihívások az ICS/SCADA világában

A cím nem saját cím, hanem egy a Magyar Víziközmű Szövetség lapjának XXVIII/2020. 2. számában, a VÍZMŰ Panoráma lapban megjelent cikknek a címe. Az említett címmel Dr. Krasznay Csaba a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Kutatóintézetének vezetője publikált egy érdekes cikket, melyben szó esik többek között arról, hogy nyilvánosan kell beszélni a Víziközművek tekintetében is a lehetséges támadások forgatókönyveiről, hogy mindenki tisztába kerülhessen a téma fontosságával.

A Stuxnet és a Digitális Mohács nem lehet ismeretlen a Black Cell ICS hírlevél rendszeres olvasóinak, Dr. Krasznay Csaba bemutatja az összefüggéseket és a Víziközmű szolgáltatók kapcsán a nyilvánosan elérhető információkat, amelyek bárki számára elérhetők a világhálón.

A szerző bemutatja a cikkben, hogy a kibertámadók miért támadtak, vagy miért támadhatnak vízi közműveket a kibertérből, ezt milyen támadással kiviztelezték vagy próbálhatják meg kivitelezni, és milyen hatások érhetők el a kibertámadások által.

A cikkben felrejlik többek között a kiberbiztonsági szakemberek által már unalomig ismert tény, hogy az admin/admin nagyon veszélyes tud lenni, vagyis az alapértelmezett felhasználónév jelszó párost minden körülmények között meg kell változtatni, függetlenül attól, hogy IT vagy OT környezetről beszélünk.

A cikkben a szerző rávilágít arra is, hogy milyen tömegkatasztrófa idézhető elő a kritikus infrastruktúrák kibertérből történő támadása által, vagy milyen adatszerzést lehet eszközölni későbbi támadás kivitelezéséhez. A támadás hibrid jellege is megjelenik a cikkben az orosz fél általi ukrán klórdesztillációs állomás támadásával.

A cikk bemutatja a Black Cell 2019-ben készült tanulmánya[1] által az ICS/SCADA rendszerek kitettségét a kibertámadásoknak, illetve a DragonFly 2.0 kampány Cyber Kill Chain-t is, melynek szakaszai:

1. Felderítés,
2. Támadó kód kialakítása,
3. Támadó kód célba juttatása,
4. Rosszindulatú kód futtatása,
5. Telepítés,
6. Irányítás és vezérlés,
7. Célokkal kapcsolatos tevékenységek.

A cikk a következő webhelyen érhető el, javasolt a víz ágazati kritikus infrastruktúrák-, és az ICS/SCADA rendszerek üzemeltetőnek az elolvasása:

http://www.maviz.org/system/files/vizmu_panorama_-_2020-2_web.pdf

[1] ICS hazai körkép (Kocsis Tamás)

ICS sérülékenységek

2020. novemberében 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:

ICSA-20-324-05: **Mitsubishi Electric MELSEC iQ-R Series**
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-324-05

ICSA-20-324-01: **Johnson Controls Sensormatic Electronics American Dynamics victor Web Client**
Magas szintű sérülékenység: nem megfelelő hitelesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-324-01

ICSA-20-324-02: **Paradox IP150**
Kritikus szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-324-02

ICSA-20-324-03: **Real Time Automation EtherNet/IP**
Kritikus szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-324-03

ICSA-20-324-04: **Schneider Electric Interactive Graphical SCADA System (IGSS)**
Magas szintű sérülékenységek: memória pufferen belüli műveletek nem megfelelő korlátozása, memória pufferen kívüli olvasás és írás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-20-324-04

ICSMA-20-317-01: **BD Alaris 8015 PC Unit and BD Alaris Systems Manager**
Közepes szintű sérülékenység: nem megfelelő hitelesítés.
https://us-cert.cisa.gov/ics/advisories/icsma-20-317-01

ICSA-20-317-01: **Mitsubishi Electric MELSEC iQ-R Series**
Közepes szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-317-01

ICSA-20-315-01: **OSIsoft PI Interface for OPC XML-DA**
Magas szintű sérülékenység: numerikus hibák.
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-01

ICSA-20-315-02: **OSIsoft PI Vision**
Magas szintű sérülékenységek: XSS, helytelen engedélyezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-02

ICSA-20-315-03: **Schneider Electric PLC Simulator for EcoStruxure Control Expert**
Magas szintű sérülékenység: szokatlan történések nem megfelelő ellenőrzése.
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-03

ICSA-20-315-04: SIMATIC S7-300 CPUs and SINUMERIK Controller
Közepes szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-04

ICSA-20-315-05: Siemens SCALANCE W 1750D
Kritikus szintű sérülékenység: nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-05

ICSA-20-252-02: Siemens SIMATIC S7-300 and S7-400 CPUs (Update B)
Közepes szintű sérülékenység: nem megfelelően védett hitelesítő adatok.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-02

ICSA-20-196-05: Siemens UMC Stack (Update C)
Közepes szintű sérülékenységek: nem jegyzett elem a keresési útvonalban, ellenőrizetlen erőforrás felhasználás, nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-310-01: WECON PLC Editor
Magas szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-310-01

ICSA-20-310-02: Mitsubishi Electric GT14 Model of GOT1000 Series
Kritikus szintű sérülékenységek: memória pufferen belüli műveletek nem megfelelő korlátozása, munkamenet rögzítés, null pointer dereferencia, nem megfelelő hozzáférés ellenőrzés, argumentum befecskendezés, erőforrás menedzsment hiba.
https://us-cert.cisa.gov/ics/advisories/icsa-20-310-02

ICSA-20-212-04: Mitsubishi Electric Factory Automation Engineering Products (Update A)
Magas szintű sérülékenység: nem jegyzett elem a keresési útvonalban.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04

ICSA-20-161-02: Mitsubishi Electric MELSEC iQ-R Series (Update B)
Közepes szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-02

ICSA-20-308-01: WAGO Series 750-88x and 750-352
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-308-01

ICSA-20-308-02: NEXCOM NIO50
Közepes szintű sérülékenységek: nem megfelelő bemeneti hitelestés, érzékeny információk egyszerű szöveges formában történő továbbítása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-308-02

ICSA-20-308-03: ARC Informatique PcVue
Kritikus szintű sérülékenységek: adat hitelességi sérülékenység, kritikus adatokhoz való nyilvános hozzáférés, érzékeny információk illetéktelenek részére történő feltárása.

https://us-cert.cisa.gov/ics/advisories/icsa-20-308-03

ICSA-20-303-01: Mitsubishi Electric MELSEC iQ-R, Q and L Series
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-303-01

ICSA-20-303-02: Mitsubishi Electric MELSEC iQ-R
Kritikus szintű sérülékenységek: memória pufferen belüli műveletek nem megfelelő korlátozása, munkamenet rögzítés, null pointer dereferencia, nem megfelelő hozzáférés ellenőrzés, argumentum befecskendezés, erőforrás menedzsment hiba.
https://us-cert.cisa.gov/ics/advisories/icsa-20-303-02

ICSA-20-282-02: Mitsubishi Electric MELSEC iQ-R Series (Update A)
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-02

ICSA-20-238-03: WECON LeviStudioU (Update B)
Magas szintű sérülékenységek: puffer túlcsordulás, nem megfelelő XML korlátozás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-238-03

ICSA-20-301-01: SHUN HU Technology JUUKO Industrial Radio Remote Control
Magas szintű sérülékenységek: hitelesítés megkerülés, parancs befecskendezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-301-01

ICSMA-20-296-01: B. Braun OnlineSuite
Magas szintű sérülékenységek: útvonal bejárás, ellenőrizetlen elem a keresési útvonalban, Excel makró befecskendezéses sérülékenység.
https://us-cert.cisa.gov/ics/advisories/icsma-20-296-01

ICSMA-20-296-02: B. Braun SpaceCom, Battery Pack SP with Wi-Fi, and Data module compactplus
Magas szintű sérülékenységek: XSS, URL nem megbízható webhelyre történő irányítása, XPath befecskendezés, munkamenet rögzítés, egyirányú sózatlan hash használata, útvonal bejárás, kriptográfiai aláírás nem megfelelő ellenőrzése, nem megfelelő privilégiumkezelés, beégetett hitelesítők használata, nem megfelelő hozzáférés ellenőrzés, aktív hibakód.
https://us-cert.cisa.gov/ics/advisories/icsma-20-296-02

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. november hónapban az ICS-CERT nem adott ki riasztást.