21. Hírlevél az ipari irányító rendszerek biztonságáról

Tisztelt Olvasó! Tájékoztatjuk, hogy az ICS biztonsági hírlevél 2021. februártól kizárólag angol nyelven fog megjelenni. A Black Cell hírlevélre feliratkozók ezentúl is havi rendszerességgel megkapják majd az *ICS security feed* hírlevelet, a honlapról letölthető formában a következő webhelyen lesz majd elérhető az ICS tudásbázis: https://blackcell.io/ics-security-feed/

Üdvözlettel: a Black Cell csapata

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

Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve

A SeConSys együttműködés az élvonalbeli magyar villamos energetikai védelmi, irányítástechnikai, kiberbiztonsági, villamosenergia termelő és szolgáltató cégek, szabályozó és felügyeleti szervezetek, valamint energetikai és kiberbiztonsági szakemberek önkéntes, nonprofit szakmai együttműködése.

A 2019-es és 2020-as években az együttműködés keretein belül elkészült egy kézikönyv az olyan villamos energia ágazati szereplők részére, akik ICS/SCADA rendszereket üzemeltetnek. A kézikönyv számos nemzetközi villamosenergia ágazati szabályozást feldolgozva, a hazai jogszabályi és egyéb előírásokat, szabványokat és ajánlásokat figyelembe véve készült, amely segítséget jelenthet a kijelölt létfontosságú rendszerelemek üzemeltetőinek a kiberbiztonság fokozásához.

Az ICS/SCADA rendszerek fenyegetettségi térképe alapján beazonosíthatók a szakterületi kockázatok, melyek napjaink egyre növekvő számú kibertámadásai során relevánsak lehetnek, így a kiberkockázatok azonosítása egyszerűbbé válhat a kézikönyv olvasói számára.

Az említett tartalmon kívül számos érdekes elemzést is tartalmaz a kézikönyv, amelyek a terület kihívásait segíthet könnyebben megérteni. A kézikönyv elolvasása ajánlott minden olyan szakértő és vezető számára, aki a villamos energia ágazatban használt ICS/SCADA rendszerek fejlesztője, gyártója, üzemeltetője, használója, biztonsági szakembere.

A Kézikönyv ingyenesen letölthető a következő webhelyről:

https://www.seconsys.eu/

ICS képzések, oktatások

A COVID-19 világjárványra tekintettel 2021. februárban 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
- Industrial IoT Markets and Security

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 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
  - 2021.02.01-06.

- ICS515: ICS Active Defense and Incident Response
  - csak márciustól

További részletek a következő webhelyen találhatók:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

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

2021. februárban a koronavírus világjárványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop virtuálisan vagy a helyszínen biztonsági intézkedések betartása mellett kerül megtartásra.

M01 Industrial Control Systems Security

A résztvevők megismerkedhetnek az ipari vezérlő rendszerek biztonsági alapjaival. Bemutatásra kerülnek incidensek, melyek az ICS rendszereket érintik, a terminológiák, továbbá esettanulmányok egyaránt.

A témát érintő fenyegetettség modellezéssel is megismerkedhet a résztvevő, illetve a releváns kockázatok elemzésével, a támadások észlelésével, védelmi módszertanokkal és jó gyakorlatokkal. A jövőbeli kihívásokat is bemutatják az előadók.

M01 Industrial Control Systems Security; (Online); 2021.02.01-05.

További információk a következő linken találhatók:

https://www.date-conference.com/tutorial/m01

Cyber Security for Critical Assets Conference

A konferencia bemutatja a MENA – Közel-Kelet és Észak-Afrika – területén elhelyezkedő kritikus infrastruktúrák védelmét. A konferencián előadnak a IT és OT biztonsági szakemberek és bemutatják, hogy miként lehet növelni a kiberbiztonsági ellenállóképességet.

Érdekes témának ígérkezik, hogy a humán tűzfal építése miként lehetséges. A mesterséges intelligencia kritikus infrastruktúra védelemben betöltött szerepe is bemutatásra kerül.

CS4CA; (Online); 2021.02.01-02.

További információk a következő linken találhatók:

https://mena.cs4ca.com/overview/

ICS üzemeltetői incidensek

Indiai áramkimaradás, amelyet valószínűleg hackerek okozhattak

2020. októberében India legnagyobb városában Mumbai-ban történt nagymértékű áramkimaradás, amelyet kibertámadás okozott. A létfontosságú szolgáltatások helyreállítása 2 órát vett igénybe, és 12 óráig tartott, míg az áramszolgáltatás helyreállt.

A kiberbiztonsági rendőrség tájékoztatása alapján nem szabotázs, hanem kibertámadás okozta az áramkimaradást. A Mumbai Mirror szerint a nyomozók több gyanús bejelentkezést találtak a szervereken, amelyek az áramellátáshoz és átviteli segédprogramokhoz kapcsolódtak. Feltételezések szerint ezeknek a szervereknek a manipulálása okozhatta a kiesést.

A tevékenység visszakövetése során dél-ázsiai országok tevékenységét sejtik a támadások mögött. A lap forrásai szerint a támadás célja a profitszerzés volt. 2020. február óta számos kibertámadást indítottak indiai áramszolgáltatók ellen, amelyek ransomware, BGP hijacking (vagyis útvonal eltérítéses), és elosztott szolgáltatás megtagadásos (DDoS) támadások voltak.

Az India Today beszámolt arról, hogy rosszindulatú programokat fedeztek fel a nyomozók egy áramelosztó központban, ahol állítólag az üzemszünet keletkezett. Az elosztóközpontok felelősek az elektromos hálózat működésének biztosításáért és monitorozásáért, valamint a villamos energia termelésének ütemezéséért és elszállításáért.

Számos olyan kiberhadsereg létezik, amelyek köztudottan villamos energia ágazati szervezeteket támadnak, ezek között van Észak-Koreához köthető csoport is.

Az áramkimaradás következtében a tömegközlekedés is megállt a nagyvárosban, megkeserítve ezzel több millió ember életét. Internetes kereséssel számos video is található, amelyen az áramkimaradás hatásait lehet figyelemmel kísérni.

A támadással kapcsolatos információk a következő linken érhetők el:

https://www.securityweek.com/major-power-outage-india-possibly-caused-hackers-reports

Szerző: keveset tudunk erről az incidensről is, sajnos nem hoznak olyan részleteket nyilvánosságra, amelyek használhatók lennének a hasonló tevékenységet folytató szervezetek számára. Azt azonban meg lehet állapítani, hogy a ransomware támadás jelen van általában minden kiberhadsereg repertoárjában, így érdemes a megelőzési tevékenységek között érdemes kiemelten foglalkozni a zsarolóvírusok elleni védelemmel.

Könyvajánló

Programmable Logic Controllers

A könyv legfrissebb 6. kiadásában a szerző kifejti a programozható logikai egységek (PLC) alapvetéseit, gyártótól függetlenül. A könyv segít megérteni a PLC-k tervezését, karakterisztikáját, belső architektúráját, az üzemeltetés alapelveit és nem utolsó sorban a biztonsági problémákat, hibaészlelési és tesztelési módszertanokat.

A legfrissebb kiadás új 1. fejezete a relével vezérelt rendszerek, a mikroprocesszorral vezérelt rendszerek és a programozható logikai vezérlők összehasonlításával foglalkozik, a PLC hardverének és architektúrájának áttekintése mellett. A könyvben megtalálható még a különböző PLC gyártók által hozott példák, IEC programozási szabvány hivatkozások, függvény diagrammok és számos esettanulmány.

Javasolt a könyv elolvasása azon személyeknek, akik a PLC üzemeltetés mélyebb rejtelmeivel is meg szeretnének ismerkedni.

Szerzők/szerkesztők: William Bolton

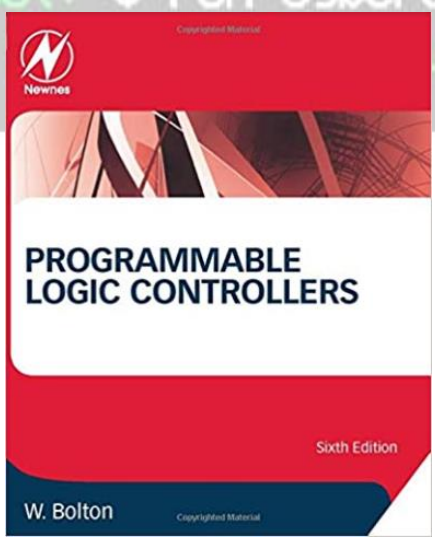
Kiadás éve: 2015.

A kiadvány elérhető a következő linken:

https://www.amazon.com/Programmable-Logic-Controllers-William-Bolton/dp/0128029293

A kiadvány 4. kiadása Pdf-ben a következő linken elérhető:

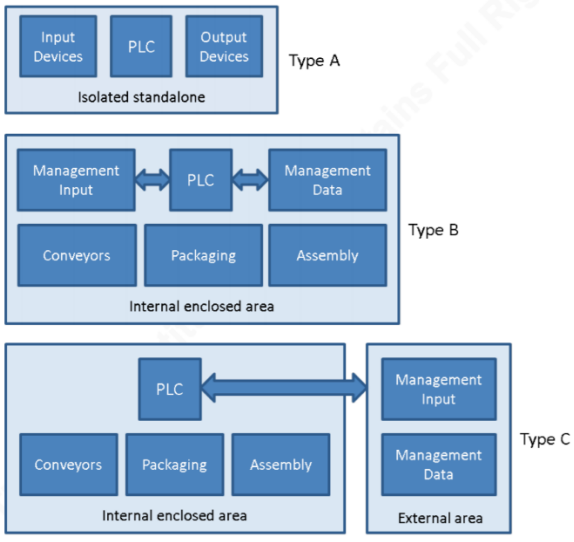
https://www.etf.ues.rs.ba/~slubura/Procesni%20racunari/Programmable%20Logic%20Controllers%204th%20Edition%20(W%20Bolton).pdf



Black Cell javaslatok

Programozható Logikai Vezérlők biztonsági igények

A SANS információbiztonsági dokumentumai közt megtalálható egy Whitepaper, amely a programozható logikai vezérlők (PLC) biztonsági kérdéseivel foglalkozik. 3 típusú modell létezik, melyek a következők:



Az „A" típus az elszigetelt önálló modell, a „B" modell a belső zárt modell és a „C" típusban a belső zárt modellhez külső menedzsment rendszer kapcsolódik.

A Whitepaper bemutatja, hogy a különböző típusú modelleket milyen fenyegetések veszélyeztetik, és milyen sérülékenységekkel kell számolni esetükben.

A PLC eszközök integritási kérdéseit is tárgyalja a dokumentum, ahogy a hitelesítési és hozzáférési kérdéseket, a kommunikáció védelmét, illetve a hálózati és rendszervédelmet. A biztonsági szint növeléséhez is állnak információk a dokumentum olvasójának rendelkezésére.

A konklúzióban megjegyzi a szerző, hogy bár a PLC egy komponense csupán az ICS rendszereknek és számos technikai elemtől függ, illetve több alkotóelemmel együtt alkot egy rendszert. Ezek az elemek technológiai és nem technológiai komponensek (például adminisztratív fizikai és logikai védelmi intézkedések), melyek együttesen fokozzák a biztonsági szintet.

További részletekért javasoljuk a Whitepaper elolvasását!

A Whitepaper a következő linken érhető el:

https://www.sans.org/reading-room/whitepapers/threats/plc-device-security-tailoring-37612

ICS sérülékenységek

2021. januárban 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-21-028-01: **Rockwell Automation FactoryTalk Linx and FactoryTalk Services Platform**
Magas szintű sérülékenységek: puffer túlcsordulás, kivételek nem megfelelő ellenőrzése és kezelése.
https://us-cert.cisa.gov/ics/advisories/icsa-21-028-01

ICSA-21-026-01: **Fuji Electric Tellus Lite V-Simulator and V-Server Lite**
Magas szintű sérülékenységek: puffer túlcsordulás, memória puffer határain kívüli olvasás és írás lehetősége, nem inicializált pointer hozzáférés.
https://us-cert.cisa.gov/ics/advisories/icsa-21-026-01

ICSA-21-007-03: **Eaton EASYsoft (Update A)**
Közepes szintű sérülékenységek: erőforrás nem kompatibilis típusú adatokhoz történő hozzáférése, memória puffer határain kívüli olvasás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-03

ICSA-20-353-01: **Treck TCP/IP Stack (Update A)**
Kritikus szintű sérülékenységek: puffer túlcsordulás, memória puffer határain kívüli olvasás és írás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-20-353-01

ICSA-20-245-01: **Mitsubishi Electric Multiple Products (Update A)**
Magas szintű sérülékenység: korábbi adatokból kiszámítható értékek.
https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01

ICSA-21-021-01: **Delta Electronics ISPSoft**
Magas szintű sérülékenység: memória felszabadítási problémák.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-01

ICSA-21-021-02: **Delta Electronics TPEditor**
Magas szintű sérülékenységek: nem megbízható (null pointer) dereferencia, memória puffer határain kívüli írás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-02

ICSA-21-021-03: **Honeywell OPC UA Tunneller**
Kritikus szintű sérülékenységek: puffer túlcsordulás, memória puffer határain kívüli olvasás lehetősége, nem megszokott körülmények nem megfelelő ellenőrzése, ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-03

ICSA-21-021-04: **Mitsubishi Electric MELFA**
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-04

ICSA-21-021-05: WAGO M&M Software fdtCONTAINER

Magas szintű sérülékenység: nem megbízható adatkezelés.

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05

ICSMA-21-019-01: Philips Interventional Workstations

Közepes szintű sérülékenység: parancs befecskendezés.

https://us-cert.cisa.gov/ics/advisories/icsma-21-019-01

ICSA-21-019-01: Dnsmasq by Simon Kelley

Magas szintű sérülékenységek: puffer túlcsordulás, az adatok hitelességének nem megfelelő ellenőrzése, kockázatos kriptográfiai algoritmus használata.

https://us-cert.cisa.gov/ics/advisories/icsa-21-019-01

ICSA-21-019-02: Reolink P2P Cameras

Kritikus szintű sérülékenységek: beégetett kriptográfiai kulcs használata, érzékeny információk egyszerű szöveges formában történő továbbítása.

https://us-cert.cisa.gov/ics/advisories/icsa-21-019-02

ICSA-20-212-03: Mitsubishi Electric Factory Automation Products Path Traversal (Update A)

Magas szintű sérülékenység: útvonal bejárás.

https://us-cert.cisa.gov/ics/advisories/icsa-20-212-03

ICSA-20-212-04: Mitsubishi Electric Factory Automation Engineering Products (Update B)

Magas szintű sérülékenység: nem jegyzett keresési út vagy elem.

https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04

ICSMA-21-012-01: SOOIL Dana Diabecare RS Products

Magas szintű sérülékenységek: beégetett hitelesítők használata, nem megfelelően védett hitelesítő adatok, helytelen véletlenszerű értékek használata, kliens oldali hitelesítés használata, szerver oldali biztonság kliens oldali érvényesítése, hitelesítés megkerülés ismétlő és hamisító módszerrel, továbbításkor nem védett hitelesítők, kulcsok kicserélése entitás hitelesítés nélkül.

https://us-cert.cisa.gov/ics/advisories/icsma-21-012-01

ICSA-21-012-01: Schneider Electric EcoStruxure Power Build-Rapsody

Magas szintű sérülékenység: veszélyes fájltípusok korlátozás nélküli feltöltésének lehetősége.

https://us-cert.cisa.gov/ics/advisories/icsa-21-012-01

ICSA-21-012-02: Siemens SCALANCE X Switches

Kritikus szintű sérülékenység: beégetett kriptográfiai kulcs használata.

https://us-cert.cisa.gov/ics/advisories/icsa-21-012-02

ICSA-21-012-03: Siemens JT2Go and Teamcenter Visualization

Magas szintű sérülékenységek: nem kompatibilis típushoz történő hozzáférés, XML külső entitások hivatkozásának nem megfelelő korlátozása, puffer túlcsordulás, null pointer dereferencia, memória puffer határain kívüli írás és olvasás lehetősége.

https://us-cert.cisa.gov/ics/advisories/icsa-21-012-03

ICSA-21-012-04: Siemens Solid Edge

Magas szintű sérülékenységek: memória puffer határain kívüli írás lehetősége, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-04

ICSA-21-012-05: Siemens SCALANCE X Products

Kritikus szintű sérülékenységek: kritikus funkció hiányzó hitelesítése, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-05

ICSA-20-196-07: Siemens Opcenter Execution Core (Update B)

Magas szintű sérülékenységek: XSS, SQL befecskendezés, nem megfelelő hozzáférés ellenőrzés, nem megfelelően védett hitelesítő adatok.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-07

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update E)

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

ICSA-20-105-06: Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update A)

Magas szintű sérülékenység: logikai hibák.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-06

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update C)

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update F)

Magas szintű sérülékenység: a puffer méretének nem megfelelő kalkulációja.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-06

ICSA-20-014-05: Siemens TIA Portal (Update B)

Magas szintű sérülékenység: útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-014-05

ICSA-19-283-02: Siemens PROFINET Devices (Update I)

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02

ICSMA-21-007-01: Innokas Yhtymä Oy Vital Signs Monitor

Közepes szintű sérülékenységek: XSS, downstream komponens által használt kimeneti speciális elemek nem megfelelő semlegesítése.
https://us-cert.cisa.gov/ics/advisories/icsma-21-007-01

ICSA-21-007-01: Hitachi ABB Power Grids FOX615 Multiservice-Multiplexer

Kritikus szintű sérülékenység: nem megfelelő hitelesítés.

https://us-cert.cisa.gov/ics/advisories/icsa-21-007-01

ICSA-21-007-02: **Omron CX-One**

Magas szintű sérülékenységek: inkompatibilis típushoz történő hozzáférés, puffer túlcsordulás, null pointer dereferencia.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-02

ICSA-21-007-03: **Eaton EASYsoft**

Közepes szintű sérülékenység: inkompatibilis típushoz történő hozzáférés, memória puffer határain kívüli olvasás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-03

ICSA-21-007-04: **Delta Electronics CNCSoft-B**

Magas szintű sérülékenységek: inkompatibilis típushoz történő hozzáférés, memória puffer határain kívüli olvasás és írás lehetősége, null pointer dereferencia.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-04

ICSA-21-005-01: **Schneider Electric Web Server on Modicon M340**

Közepes szintű sérülékenységek: memória puffer határain kívüli olvasás és írás lehetősége, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-01

ICSA-21-005-02: **Panasonic FPWIN Pro**

Magas szintű sérülékenység: memória puffer határain kívüli olvasás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-02

ICSA-21-005-03: **GE Reason RT43X Clocks**

Kritikus szintű sérülékenységek: kód befecskendezés, beégetett kriptográfiai kulcs használata.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-03

ICSA-21-005-04: **Red Lion Crimson 3.1**

Magas szintű sérülékenységek: null pointer dereferencia, kritikus funkció hiányzó hitelesítése, nem megfelelő erőforrás leállítás.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-04

ICSA-21-005-05: **Delta Electronics DOPSoft**

Magas szintű sérülékenységek: memória puffer határain kívüli írás lehetősége, nem megbízható (null pointer) dereferencia.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-05

ICSA-21-005-06: **Delta Electronics CNCSoft ScreenEditor**

Magas szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-06

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

2021. január hónapban az ICS-CERT nem adott ki riasztást.