18. 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

Kibertervezés, reagálás és helyreállítás

Az Egyesült Államok Szövetségi Energetikai Szabályozó Bizottsága (FERC) és az Észak-Amerikai villamosenergetikai társaság (North American Electricity Reliability Corporation – NERC) 2020. szeptemberében publikálta a „Cyber Planning for Response and Recovery Study" című tanulmányát, mely a kiberincidensekre történő reagálás és az incidenskezelés legjobb gyakorlatait foglalja össze.

A kiadvány elkészítésében nyolc Egyesült Államokbeli villamosenergiai vállalat nyújtott segítséget. A villamosenergia-szolgáltatás kiesése szerte a világban számos negatív hatással jár, és dominó elvszerűen ágazatról ágazatra gyűrűzik tovább. Emiatt javasolt az üzemeltetőknek a jó gyakorlatokat áttekinteni, és a más szervezetek által elkövetett hibákból tanulva a jó gyakorlatokat a saját incidensmenedzsment rendszerébe beépíteni.

A szerzők célja egy olyan ajánlásgyűjtemény kidolgozása volt, amely segítséget nyújt az egyedi incidenskezelési és -helyreállítási tervek kidolgozásában, az egyedi működési és egyéb sajátosságok figyelembevétele mellett.

A tanulmányban az IT és OT biztonság, az e-mail és közösségi média hozzáférési kérdések, továbbá az internettel kapcsolatba kerülő rendszerelemek is tárgyalásra kerülnek. A dokumentum az „Esemény" és „Incidens" fogalmakba és értelmezésükbe, valamint az incidenskezelési eljárásrendek felépítésének gyakorlatába és folyamatába is betekintést nyújt.

Az erőforrás-tervezésre nagy hangsúlyt fektet a tanulmány. Az események és incidensek egyedisége miatt számos meglepetés érhet egy szervezetet, azonban megfelelő erőforrás-menedzsmenttel a nem várt események hatásai nagymértékben csökkenthetők. Egy incidens okozta kár a legtöbb esetben magasabb költséget okoz egy szervezetnek, mint a védelemre szánt összeg, és emellett további negatív hatásokkal kell szembesülni egy incidens esetén, mint például a bizalom- és/vagy reputációvesztés.

A tanulmányról részletesebb információkhoz jutni a következő linken található cikkből lehet:

https://securityaffairs.co/wordpress/108573/ics-scada/ferc-nerc-cyber-incident-response.html

A tanulmány a következő linken érhető el:

https://cms.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf

ICS képzések, oktatások

A COVID-19 világjárványra tekintettel 2020. novemberben 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 kurzusok végezhetők el:

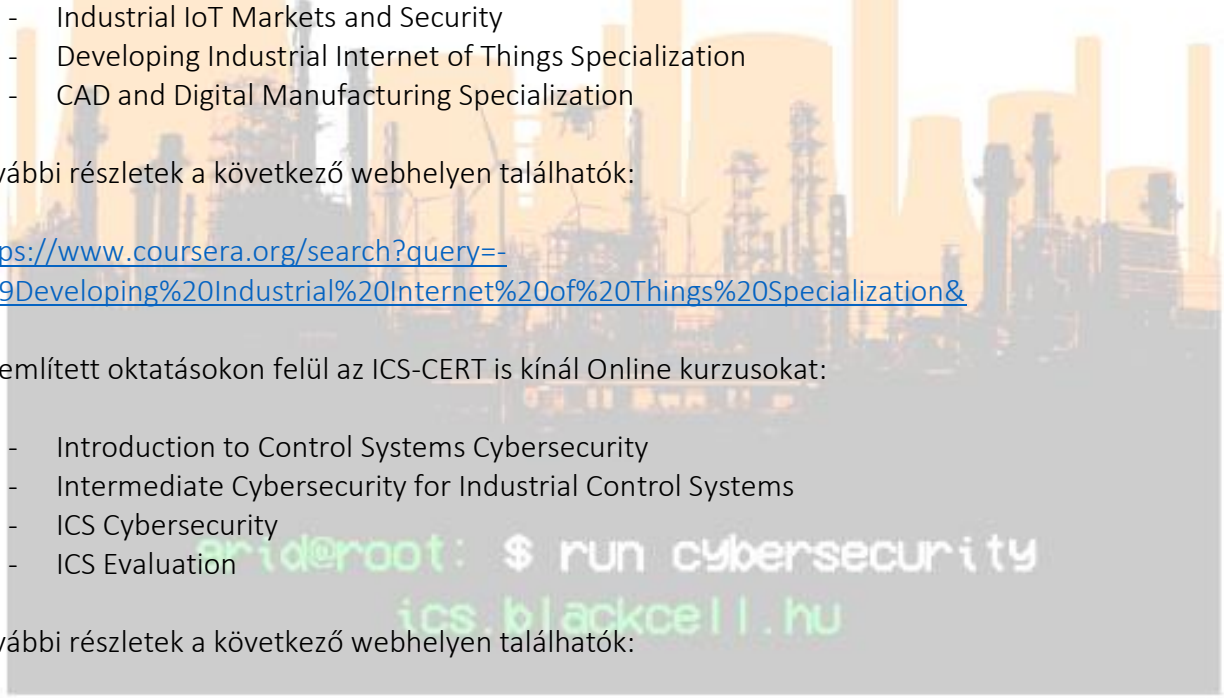
- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization
- CAD and Digital Manufacturing Specialization

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
  - 2020.11.2-7. (két külön instruktorral)
  - 2020.11.14-19.
  - 2020.11.16-21. (két külön instruktorral)

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

7th Annual Industrial Control Cyber Security Europe

A 7. ipari irányítási kiberbiztonsági konferenciát az online térben rendezi meg a CyberSenate. A konferencián az integrált OT technológiák elterjedése miatti hatékonyság növelés mellett szó lesz az ellenállóképesség csökkenéséről és a növekvő támadási felületekről.

Két kulcskérdés került előzetesen megfogalmazásra a konferencián:

- Milyen módon lehet biztosítani az innováció megbízhatóságát és biztonságát?
- Az ágazati vezetők miként definiálják az Ipar 4.0 ellenállóképességet?

7th Annual Industrial Control Cyber Security Europe; (Online konferencia, Egyesült Királyság); 2020.11.03-04.

További információk a következő linken találhatók:

https://icseurope.pathable.co/

APAC ICS Summit & Training 2020

A SANS szervezésében online kerül megrendezésre a 2020-as esztendőben az APAC ICS Summit & Training 2020. A november 13-i online ICS rendszerek biztonságáról szóló találkozón ingyenesen részt vehetnek, akik regisztrálnak!

A konferencián lesznek magas technikai szintű előadások, élő demók és esettanulmányok is, mind támadói, mind védelmi szemszögből. Az oktatás része a rendezvénynek már fizetős, ám a szakma nagyágyúi tartanak előadásokat és nem utolsó sorban 8 CPE ponttal gazdagodhat, aki részt vesz az eseményen!

APAC ICS Summit & Training 2020; (Online konferencia, Szingapúr); 2020.11.13. és 2020.11.16-21.

További információk a következő linken találhatók:

https://www.sans.org/event/ics-asia-pacific-2020

ICS üzemeltetői incidensek

A 17. ICS hírlevélben bemutatott pakisztáni zsarolóvírus támadás utóélete

A pakisztáni Karacsi városának áramszolgáltatóját (K-Electric) zsarolóvírus-támadás érte, melyet a Netwalker nevű zsarolóvírussal követtek el a támadók. A 17. ICS hírlevélben bemutattuk, hogy a támadók váltságdíjat követeltek, hogy a titkosítatlanul ellopott fájlokat visszaszolgáltassák.

A Bleepingcomputer cikkéből kiderült, hogy a K-Electric nem fizetett a támadóknak, és azt nyilatkozta a cég a Bleepingcomputernek, hogy nem loptak el semmilyen adatot a szervezettől.

Azonban a Netwalker publikálta az ellopott 8,5 Gb adatot, és az a szakértők szerint tartalmazott pénzügyi adatokat, vásárlói információkat, mérnöki jelentéseket, karbantartási naplókat és egyebeket. Az adatok tartalmaztak nem auditált eredmény-kimutatásokat, a turbinák műszaki ábráit és a vásárlói nyilatkozatok képeit, amelyek a K-Electric-től származnak. A műszaki ábrák alkalmasak egy későbbi ICS támadás előkészítéséhez, és annak további információigényének meghatározásához.

Nem elhanyagolható szempont, hogy az ügyfelek aggódnak saját személyes adataik szervezettől történő kikerülése miatt. Ez reputációs veszteség a cégnek, amely pénzügyi veszteségbe is átcsaphat. A Bleepingcomputer kereste a szervezetet további információkért, azonban a szervezet már nem válaszolt ezekre.

Szakértői szemmel érthetetlen, hogy bizonyos szervezetek miért próbálják titkolni ilyen esetben, hogy mi történt, és miért nem adnak tájékoztatást az érintettek részére, hogy az adataikat rosszindulatú támadók ellopták. Így mindenki számára világos lenne a helyzet, és esetleg fel tud készülni a negatív hatásokra adott személy/szervezet, vagy esetleg védelmi intézkedéseket tud foganatosítani. Az utólag kiderülő titkolózás sokkal nagyobb károkat tud okozni közvetve és közvetlenül is!

Nem szégyen az, ha valaki kibertámadás áldozatává válik. Minden szervezet sebezhető, idő kérdése megtalálni a sérülékenységeket a támadóknak. Az viszont már minősít egy szervezetet, hogy ilyen helyzetben miként reagál. A világos kommunikáció az érintett felek részére alapvető elvárás, ahogy az incidenst követő remediációs cselekmények megtétele is.

További információk az incidenssel kapcsolatban az alábbi linken találhatók:

https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/

Könyvajánló

Az ipari rendszerek kiberbiztonsága napjainkban kulcsfontosságú kérdés.

A releváns megoldások megvalósításához az iparban dolgozó vezetőnek tisztában kell lenni az informatikai rendszerekkel, a kommunikációs hálózatokkal és az irányító rendszerekkel. Bizonyos tudással kell rendelkezzenek a támadók technikáiról, a vonatkozó szabványokról és előírásokról, és az elérhető védelmi megoldásokról.

A könyv az előzőekben említett tényezőket mutatja be, és áttekintést biztosít az ipari rendszerek kiberbiztonságát illetően. A szerző a klasszikus SCADA rendszerek, valamint az IIoT vagyis az Industrial Internet of Things – ipari dolgok internete – tekintetében is foglalkozik a kiberbiztonság kérdéseivel.

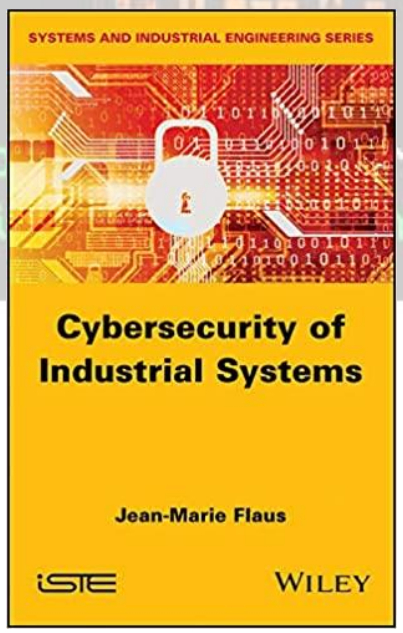
A könyv címe: **Cybersecurity of Industrial Systems**

Szerzők/szerkesztők: Jean-Marie Flaus

Kiadás éve: 2019.

A kiadvány elérhető a következő linken:

https://www.amazon.com/Cybersecurity-Industrial-Systems-Engineering/dp/178630421X/ref=pd_sbs_14_5/139-2402915-3452033?_encoding=UTF8&pd_rd_i=178630421X&pd_rd_r=a874f3f8-71c2-4eb6-8de8-6cb697e433f7&pd_rd_w=rRx7u&pd_rd_wg=qWzQR&pf_rd_p=b65ee94e-1282-43fc-a8b1-8bf931f6dfab&pf_rd_r=V5W2SN95937KG5R233BR&psc=1&refRID=V5W2SN95937KG5R233BR



Black Cell javaslatok

Az ipari irányító rendszerek fenyegetései

Annak érdekében, hogy megfelelően ellenálló kiberbiztonsági rendszert építhessen ki egy ICS rendszert üzemeltető szervezet, mindenképpen ismernie kell a fenyegetések történetét, fejlődését, illetve természetét.

A fenyegetettségi térkép akkor lesz teljeskörű, ha a kezdetektől tisztában vagyunk az ICS rendszereket ért támadásokkal, azok okaival, a támadás elkövetőjével (vagy feltételezett elkövetőjével), a támadási módszerekkel és a következményekkel. Ennek megismeréséhez Kevin E. Hemsley és Dr. Ronald E. Fisher nyújthat segítséget, „History of Industrial Control System Cyber Incidents" című kiadványával.

A dokumentum az 1903-ban történt nagy vezetéknélküli hekkelés történetével indítja a fenyegetések sorát, Macroni telegráf morse kóddal történő hekkelésének bemutatásával. Bemutatásra kerülnek a szakmában klasszikusnak számító Stuxnet, Black Energy, Shamoon, NotPetya, ukrán villamos energia rendszer elleni támadások, továbbá a Night Dragon, Havex és egyéb incidensek.

A kritikus infrastruktúrák között is létfontosságú villamos energia rendszerek elleni támadásokon kívül részletezi a dokumentum a gázellátó rendszerek, víz ágazati rendszerek, pénzügyi rendszerek elleni támadásokat is, ahol ICS rendszerek voltak érintettek a támadásokban, egészen 2018-ig bezárólag.

A dokumentum elolvasása által kialakulhat az ICS rendszerek fenyegetettségi térképe, amely a már megtörtént incidensek elemzésével tárható fel. Természetesen a támadók mindig újabb módszerekkel is próbálkoznak az ICS rendszerek elleni támadások kivitelezésére, azonban a régi jól bevált recept is sokszor előkerül, mint lehetőség.

Az ICS rendszer üzemeltetőknek meg kell tudni határozni a fenyegetettségi térkép alapján, hogy milyen fenyegetéseknek vannak kitéve a saját ágazatukban, milyen motivációjú támadók, milyen módszerekkel támadhatják a rendszereket.

A dokumentum konklúzió részében kifejtésre kerül, hogy az IoT (a dolgok internete – Internet of Things) elterjedése miatt a kiberbiztonság garantálása egyre bonyolultabbá válik, és a kritikus infrastruktúrák üzemeltetőitől kiemelt figyelmet igényel az ICS rendszerek védelme. A támadók egyre szofisztikáltabb módszerekkel támadnak, és egyre inkább rendelkeznek a megfelelő tudásszinttel és erőforrásokkal a támadások kivitelezését illetően. Emiatt a felhasználható, rendelkezésre álló információk kiemelt jelentőséggel bírnak.

A dokumentum a következő linken érhető el:

https://www.osti.gov/servlets/purl/1505628

ICS sérülékenységek

2020. októberében 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-20-294-01: **Rockwell Automation 1794-AENT Flex I/O Series B**
Magas szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-294-01

ICSA-20-294-02: **Hitachi ABB Power Grids XMC20 Multiservice-Multiplexer**
Kritikus szintű sérülékenység: nem megfelelő hitelesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-294-02

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

ICSMA-20-196-01: **Capsule Technologies SmartLinx Neuron 2 (Update A)**
Magas szintű sérülékenység: védelmi mechanizmus hiba.
https://us-cert.cisa.gov/ics/advisories/icsma-20-196-01

ICSA-20-289-01: **Advantech WebAccess/SCADA**
Magas szintű sérülékenység: fájlnév vagy útvonal külső ellenőrzése.
https://us-cert.cisa.gov/ics/advisories/icsa-20-289-01

ICSA-20-289-02: **Advantech R-SeeNet**
Magas szintű sérülékenység: SQL befecskendezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-289-02

ICSA-20-203-01: **Wibu-Systems CodeMeter (Update C)**
Kritikus szintű sérülékenységek: puffer kezelési hiba, nem megfelelő erősségű titkosítás, eredet érvényességi hiba, nem megfelelő bemeneti hitelesítés, kriptográfiai aláírás helytelen ellenőrzése, az erőforrások nem megfelelő leállítása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

ICSA-20-287-01: **MOXA NPort IAW5000A-I/O Series**
Kritikus szintű sérülékenységek: munkamenet rögzítés, nem megfelelő privilégium menedzsment, gyenge jelszó elvárások, érzékeny információk egyszerű szöveges formában történő továbbítása, túlzott próbálkozási kísérletek nem megfelelő korlátozása, érzékeny információk feltárása nem jogosultak számára.
https://us-cert.cisa.gov/ics/advisories/icsa-20-287-01

ICSA-20-287-02: **LCDS LAquis SCADA**
Magas szintű sérülékenység: memória puffer határain kívüli olvasás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-20-287-02

ICSA-20-287-03: Flexera InstallShield

Magas szintű sérülékenység: nem megbízható keresési útvonal.
https://us-cert.cisa.gov/ics/advisories/icsa-20-287-03

ICSA-20-287-04: Fieldcomm Group HART-IP and hipserver

Kritikus szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-287-04

ICSA-20-287-05: Siemens Desigo Insight

Közepes szintű sérülékenységek: SQL befecskendezés, a felhasználói felület rétegeinek vagy kereteinek nem megfelelő korlátozása, érzékeny információk feltárása nem jogosultak számára.
https://us-cert.cisa.gov/ics/advisories/icsa-20-287-05

ICSA-20-287-06: Siemens SIPORT MP

Magas szintű sérülékenység: ügyféloldali hitelesítés alkalmazása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-287-06

ICSA-20-252-02: Siemens SIMATIC S7-300 and S7-400 CPUs (Update A)

Közepes szintű sérülékenység: nem megfelelően védett hitelesítő adatok.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-02

ICSA-20-252-07: Siemens Industrial Products (Update A)

Közepes szintű sérülékenység: érzékeny információk feltárása nem jogosultak számára.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

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

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

ICSA-17-332-01: Siemens SCALANCE W1750D, M800, S615, and RUGGEDCOM RM1224 (Update C)

Magas szintű sérülékenységek: ellenőrizetlen erőforrás felhasználás, memória puffer határain belüli műveletek nem megfelelő korlátozása.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-332-01

ICSA-20-282-01: Johnson Controls Sensormatic Electronics American Dynamics victor Web Client

Magas szintű sérülékenység: nem megfelelő engedélyezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-01

ICSA-20-282-02: Mitsubishi Electric MELSEC iQ-R Series

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-02

ICSA-20-203-01: Wibu-Systems CodeMeter (Update B)

Kritikus szintű sérülékenységek: puffer kezelési hiba, nem megfelelő erősségű titkosítás, eredetellenőrzési hiba, nem megfelelő bemeneti hitelesítés, kriptográfiai aláírás helytelen ellenőrzése, nem megfelelő erőforrás leállítás.

https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

ICSA-20-273-01: MB Connect line mbCONNECT24, mymbCONNECT24
Kritikus szintű sérülékenységek: SQL befecskendezés, CSRF, parancs befecskendezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-273-01

ICSA-20-273-02: Yokogawa WideField3
Alacsony szintű sérülékenység: puffer kezelési hiba.
https://us-cert.cisa.gov/ics/advisories/icsa-20-273-02

ICSA-20-273-03: B&R Automation SiteManager and GateManager
Magas szintű sérülékenységek: útvonal bejárás, ellenőrizetlen erőforrás felhasználás, információ feltárás, nem megfelelő hitelesítés, információ kitettség.
https://us-cert.cisa.gov/ics/advisories/icsa-20-273-03

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