12. 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 Európai Unió Hálózat és Információbiztonsági Ügynöksége (ENISA) 2020. április 6-án megjelentetett egy eszközt, amely a nemzetközi biztonsági szabványokkal és ajánlásokkal fennálló összefüggések feltérképezésére alkalmas. Az eszköz a következő linken érhető el: https://www.enisa.europa.eu/topics/nis-directive/Interdependencies_OES_and_DSPs

Az ENISA még 2018-ban kiadott egy riportot, amely elemzi az alapvető szolgáltatást nyújtók és a digitális szolgáltatók összefüggéseit, és mutatószámokat ad azok értékeléséhez. A riport a következő linken érhető el: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps

A mutatók a következő szabványokhoz és ajánlásokhoz kerültek hozzárendelésre: ISO IEC 27002, COBIT5 és NIST Cybersecurity Framework.

A létfontosságú szolgáltatások napjainkban egyre jobban függenek a digitális szolgáltatásoktól, és az összefüggések kockázatmenedzsment során történő értékelésében (különösen az ágazatok közötti és a határokon átívelő függőségek tekintetében) az ENISA által kiadott eszköz nagy segítséget nyújthat. Az eszköz a NIS irányelvnek való megfeleléshez is hozzájárul, a közös és konvergens biztonsági szint uniós szintű elérése érdekében.

Az értékelés folyamatát a következő ábra szemlélteti:

Az eszköz használata segítséget nyújt az összefüggések feltérképezésében az alapvető szolgáltatások és a digitális szolgáltatások vonatkozásában, támogatja a kockázatmenedzsment folyamatokat (összefüggések hatásainak és kockázatainak értékelése), továbbá szolgálja a szabványoknak és ajánlásoknak történő megfelelést.

További információ a következő linken érhető el:

https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-a-tool-for-the-mapping-of-dependencies-to-international-standards

ICS képzések, oktatások

A teljeség igénye nélkül 2020. májusban, ICS biztonság tárgyában a következő tréningek, oktatások kerülnek lebonyolításra:

2020. májusban a SANS a COVID-19 világjárványra tekintettel kizárólag online formában tart ICS képzéseket, oktatásokat, amelyekről 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 videós 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. 06. 15 – 19. Ezt követően a következő kurzus 2020. augusztusban 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. májusban a koronavírus járványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop vagy elmarad, vagy valamely későbbi időpontra kerül megrendezésre.

A korábban meghirdetett 2020. májusi ICS és SCADA biztonsági konferenciák elhalasztott időpontjai a honlapok változása-, vagy elérhetetlensége miatt nem állapíthatók meg teljes biztonsággal, emiatt majd az aktuális ICS biztonsági hírlevélben adunk ezekről tájékoztatást.

Javasoljuk a konferenciák helyett a webinárok és oktató videók megtekintését, mely jelen helyzetben célravezető!

Változás esetén információkat megosztjuk a hírlevélre feliratkozókkal.

ICS incidensek

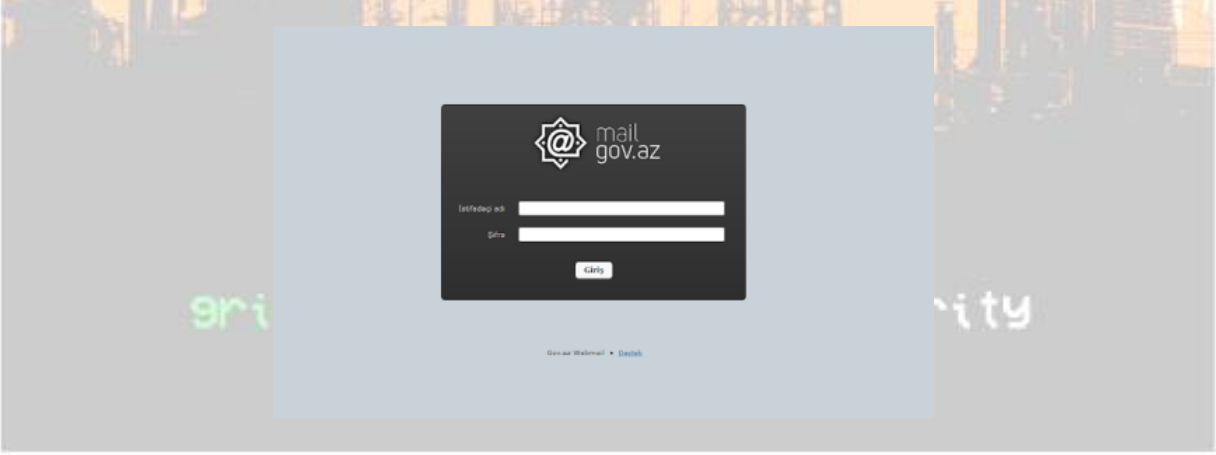
Koronavírus témájú kampány az energia ágazati szereplők ellen Azerbajdzsánban

A Cisco Talos biztonsági kutatói fedezték fel az új malware kampányt, amely a PoetRAT trójai segítségével valósítható meg. A támadás az azerbajdzsáni kormányt és a közüzemi vállalatokat célozta meg a SCADA rendszerek megfertőzésével, amelyeket széles körben használnak az energiaszektorban és a feldolgozóiparban.

A támadás során az azerbajdzsáni kormány megszemélyesítésével küldtek rosszindulatú programokat olyan URL-ekkel, amelyek a későbbiekben SCADA üzemeltetőket céloztak (többek között szélturbina rendszereket). A szakértők szerint ismert (orosz) kibertámadók állnak a támadások mögött.

A rosszindulatú programokkal fertőzött ICS és SCADA rendszerek a megújulóenergia-szektort érintették elsősorban. A támadók adathalász támadásokat indítottak Word dokumentumok felhasználásával. A szakértők három külön adathalász támadást azonosítottak, amelyek használták a COVID19-et, mint napjainkban rendkívüli érdeklődésre számot tartó tényezőt.

Az üzenetekben a „C19.docx” nevű dokumentumot használták, mely az áldozatok állítása szerint az azerbajdzsáni kormánytól és az Indiai Védelmi Minisztériumtól származtak. A támadás két komponensből állt, a támadás detektálásának megnehezítése érdekében. A káros kód ellenőrzi, hogy sandboxban fut-e (makró ellenőrzi, hogy a meghajtó nagyobb-e 62 GB-nál), és amennyiben ezt észleli, törli saját magát.



A híradások a támadások hatásait nem részletezik, inkább a támadások tényét, és technikai részleteit teszik közzé, a még nyilvánosság által is megismerhető módon.

A kampány további részleteit a következő webhelyeken ismerheti meg:

https://www.securityweek.com/hackers-targeting-azerbaijan-show-interest-scada-systems?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29

https://securityaffairs.co/wordpress/101837/hacking/poetrat-trojan-coronavirus.html

Könyvajánló

A **Power System SCADA and Smart Grids** c. könyv bemutatja az ipari automatizáció történetét, a SCADA rendszerek felépítését, komponenseit, alkalmazásait, alapvető funkcióit. A SCADA rendszerek előnyei szintén kifejtésre kerülnek az energia ágazatban, illetve a szállító és elosztó rendszerekben betöltött szerepe is.

Részletesen bemutatásra kerülnek a távolról elérhető egységek (RTU), és az ember-gép interfészek (HMI) működési és működtetési szempontból, továbbá a kapcsolódó protokollok, illetve kapcsolódó intelligens elektronikus eszközök.

A biztonság szempontjából kiemelten fontos riasztások és értesítések is részleteiben bemutatásra kerülnek, hardver és szoftver kapcsolódások szintjén egyaránt. SCADA biztonsággal kapcsolatos esettanulmányokat is bemutatnak a szerzők.

A SCADA topológiák, mobil eszköz kapcsolatok, kommunikációs módok, az alállomások és további Energia Menedzsment Rendszerek is részleteiben tanulmányozhatók a könyv elolvasásával.

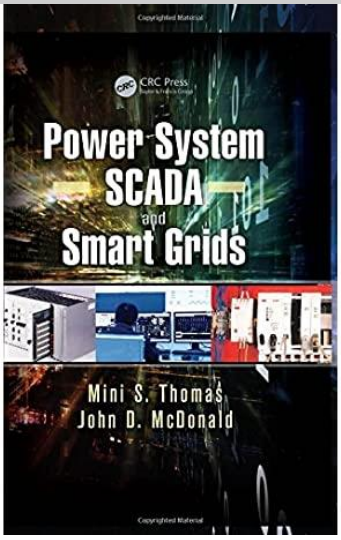
A könyv címe: **Power System SCADA and Smart Grids**

Szerzők: Mini S. Thomas, John Douglas McDonald

Kiadás éve: 2015.

A kiadvány elérhető a következő linken:

https://books.google.hu/books?hl=hu&lr=&id=wnN3CAAAQBAJ&oi=fnd&pg=PP1&dq=SCADA+security+ebook&ots=nSsqWa1JVf&sig=oclY8JChoARnQI4SFW0VBf6R_uk&redir_esc=y#v=onepage&q&f=false



Szerző: Az ICS és a SCADA biztonság megteremtéséhez elengedhetetlen a rendszerek felépítésének pontos ismerete részletekbe menően. A könyv kiváló alapot nyújt az energiaszektorban használt rendszerek megismeréséhez, és az ellenállóképesség kialakításához!

Black Cell javaslatok

A COVID-19 járványra tekintettel elengedhetetlenül is nagyobb szerep hárul az automatizációra és a digitalizációra. Rengeteg ipari irányító rendszerhez nagyobb szükség van a távoli elérésre napjainkban, mint eddig bármikor. Ahhoz, hogy a rendelkezésre állás ne sérüljön, és az ICS rendszerek megfelelő működése biztosított lehessen, rengeteg tényezőre szükséges figyelmet szentelni, beleértve a távoli elérés biztonságának szavatolását is.

A távoli elérésekkel kapcsolatos biztonságról többet tudhat meg, ha ellátogat a Black Cell tematikus weboldalaira:

https://blackcell.hu/pandemia-ipari-taveleres-vpn/
https://blackcell.hu/pandemia-tavmunka-vedelem/
https://blackcell.hu/pandemia-tavmunka-vedelem/#VPN

A távoli elérések menedzsmentjét ma már számos megoldás biztosíthatja. Ezek közül minden szervezet a kompatibilis, és költségarányos megoldásokat választja. A TeamViewer kiváló megoldás a távoli elérések menedzselésére, mely mobileszközökön, Windows, Linux vagy MacOS eszközökön is kiválóan működik.

A TeamViewer megoldással kapcsolatos további információkért látogasson el weboldalunkra:

https://blackcell.hu/teamviewer/

A különböző távoli elérésekkel kapcsolatos megoldások azonban bármely rendszerbe implementálva sérülékenységeket rejthetnek magukban, vagy keletkeztethetnek, melynek számos oka lehet. A régebbi-, vagy frissítetlen rendszerekbe implementált megoldások a rendszer más elemei által is sérülékennyé válhatnak, illetve a nem megfelelően konfigurált megoldások szintén támadási felületeket nyithatnak a kibertámadók részére.

A sérülékenységvizsgálat ebben a helyzetben elengedhetetlen, hogy ezek a sérülékenységek feltárásra és befoltozásra kerüljenek, hogy a távmunka biztonságos lehessen. A sérülékenységvizsgálattal kapcsolatos további információkat a weboldalunkon találhat:

https://blackcell.hu/pandemia-serulekenyseg-vizsgalat/

A távmunkát lehetővé tevő alkalmazások és megoldások ellenőrzése szintén kiemelkedő figyelmet kell, hogy kapjanak. Enélkül nem lehetséges a magas rendelkezésre állás biztosítása. A monitoringgal kapcsolatos további információkat a weboldalunkon talál:

https://blackcell.hu/pandemia-tavmunka-monitoring/

A logikai sérülékenységek mellett azonban fizikai és adminisztratív hiányosságok is gátolhatják az ellenálló ICS rendszerek folyamatos működését. Ezért a kockázatokat fel kell mérni, elemezni kell és az elfogadhatatlan mértékű kockázatokat kezelni kell. A kockázatmenedzsmenttel kapcsolatos további információkat a weboldalunkon találja meg:

https://blackcell.hu/pandemia-kockazatmenedzsment/

ICS sérülékenységek

2020. áprilisban 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-19-122-03: **Sierra Wireless AirLink ALEOS (Update B)**
Kritikus szintű sérülékenységek: parancs befecskendezés, beégetett hitelesítő használat, nem megfelelő fájlok feltöltésének lehetősége, XSS, CSRF, információ feltárás, érzékeny adatok hiányzó titkosítása.
https://www.us-cert.gov/ics/advisories/ICSA-19-122-03

ICSA-20-112-01: **Inductive Automation Ignition**
Kritikus szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-112-01

ICSA-20-105-01: **Eaton HMiSoft VU3**
Magas szintű sérülékenységek: puffer túlcsordulás, puffer határain kívüli olvasás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-20-105-01

ICSA-20-105-02: **Triangle MicroWorks DNP3 Outstation Libraries**
Magas szintű sérülékenység: puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-20-105-02

ICSA-20-105-03: **Triangle MicroWorks SCADA Data Gateway**
Kritikus szintű sérülékenységek: puffer túlcsordulás, puffer határain kívüli olvasás lehetősége, erőforráshoz történő inkompatibilis hozzáférés lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-20-105-03

ICSA-20-105-04: **Siemens Climatix**
Közepes szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-20-105-04

ICSA-20-105-05: **Siemens IE/PB-Link, RUGGEDCOM, SCALANCE, SIMATIC, SINEMA**
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás, nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-105-05

ICSA-20-105-06: **Siemens SIMOTICS, Desigo, APOGEE, and TALON**
Magas szintű sérülékenység: eszköz IP cím változtatási lehetőség (logikai hiba).
https://www.us-cert.gov/ics/advisories/icsa-20-105-06

ICSA-20-105-07: **Siemens SCALANCE & SIMATIC**
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-105-07

ICSA-20-105-08: **Siemens KTK, SIDOOR, SIMATIC, and SINAMICS**

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-105-08

ICSA-20-105-09: Siemens TIM 3V-IE and 4R-IE Family Devices
Kritikus szintű sérülékenység: jogosulatlanok számára is engedélyezett és aktív hibakeresési kód alkalmazása.
https://www.us-cert.gov/ics/advisories/icsa-20-105-09

ICSA-20-042-05: Siemens SIMATIC S7 (Update B)
Közepes szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-042-05

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update B)
Magas szintű sérülékenység: puffer méret nem megfelelő számítása.
https://www.us-cert.gov/ics/advisories/icsa-20-042-06

ICSA-20-014-05: Siemens TIA Portal (Update A)
Magas szintű sérülékenység: útvonal bejárás.
https://www.us-cert.gov/ics/advisories/icsa-20-014-05

ICSA-19-283-02: Siemens PROFINET Devices (Update E)
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-283-02

ICSA-19-253-03: Siemens Industrial Products (Update F)
Magas szintű sérülékenységek: értékkezelési hiba, ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-253-03

ICSA-20-100-01: Rockwell Automation RSLinx Classic
Magas szintű sérülékenység: kritikus erőforrás engedélyezési hibája.
https://www.us-cert.gov/ics/advisories/icsa-20-100-01

ICSA-20-098-01: Advantech WebAccess/NMS
Kritikus szintű sérülékenységek: kontrollálatlan fájl feltöltés, SQL befecskendezés, útvonal bejárás, kritikus funkció hiányzó hitelesítése, nem megfelelő XML korlátozás, parancs befecskendezés.
https://www.us-cert.gov/ics/advisories/icsa-20-098-01

ICSA-20-098-02: GE Digital CIMPLICITY
Közepes szintű sérülékenység: nem megfelelő privilégium menedzsment.
https://www.us-cert.gov/ics/advisories/icsa-20-098-02

ICSA-20-098-03: HMS Networks eWON Flexy and Cosy
Közepes szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-20-098-03

ICSA-20-098-04: Fuji Electric V-Server Lite
Magas szintű sérülékenység: puffer túlcsordulás.

https://www.us-cert.gov/ics/advisories/icsa-20-098-04

ICSA-20-098-05: KUKA.Sim Pro
Alacsony szintű sérülékenység: az üzenet integritásának sérülése adattovábbítás során.
https://www.us-cert.gov/ics/advisories/icsa-20-098-05

ICSA-20-042-01: Synergy Systems & Solutions HUSKY RTU (Update A)
Kritikus szintű sérülékenységek: nem megfelelő azonosítás és hitelesítés, kritikus funkció hiányzó hitelesítése, nem megfelelő kivétel ellenőrzés, helytelen alapengedélyek, szenzitív információk feltárása.
https://www.us-cert.gov/ics/advisories/icsa-20-042-01

ICSA-20-093-01: B&R Automation Studio
Magas szintű sérülékenységek: nem megfelelő privilégium menedzsment, kriptográfia hiánya, útvonal bejárás.
https://www.us-cert.gov/ics/advisories/icsa-20-093-01

ICSMA-20-091-01: BD Pyxis MedStation and Pyxis Anesthesia (PAS) ES System
Közepes szintű sérülékenység: védelmi mechanizmus hibája.
https://www.us-cert.gov/ics/advisories/icsma-20-091-01

ICSA-20-091-01: Hirschmann Automation and Control HiOS and HiSecOS Products
Kritikus szintű sérülékenység: puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-20-091-01

ICSA-20-091-02: Mitsubishi Electric MELSEC
Közepes szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-091-02

ICSA-20-016-01: Schneider Electric Modicon Controllers (Update A)
Magas szintű sérülékenység: nem megfelelő kivétel kezelés.
https://www.us-cert.gov/ics/advisories/icsa-20-016-01

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. április 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