13. Hírlevél az ipari irányító rendszerek biztonságáról

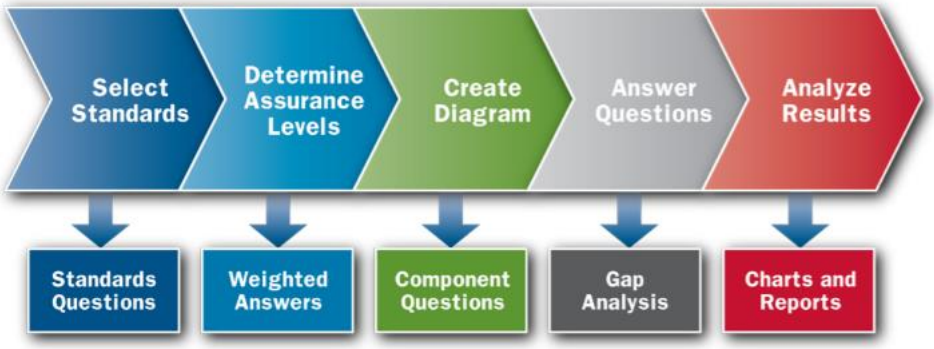
A Black Cell elkötelezett az ipari irányító rendszerek (Industrial Control Systems – ICS), és/vagy kritikus infrastruktúrák biztonságának megteremtésében, ezért havonta hírlevelet bocsát ki a témában. A hírlevélben az érintett szervezetek, illetve kritikus infrastruktúra üzemeltetők tájékozódhatnak, 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

Cyber Security Evaluation Tool (CSET)

Az Egyesült Államok Belbiztonsági Minisztérium részeként működő ICS-CERT fejlesztett egy olyan szoftvert, amely segítséget nyújt az IT és ICS rendszerek érettségi szintjének megállapításához, és különböző szabványoknak és ajánlásoknak történő megfeleléshez (ezek közül talán a legismertebb a NIST SP 800-53 r4, és a NIST SP 800-82 r2).



A fenti ábra mutatja a folyamatot, amely segít megállapítani az érettségi szintet. Lehetőség van kiválasztani a szabványt, ajánlást, amelynek meg kíván felelni a szervezet. A Cyber Security Evaluation Tool (CSET) eredményterméke egy olyan ajánlás lista, amely priorizált formában tartalmazza a megfeleléshez szükséges ajánlott intézkedések listáját.

A CSET használatának előnyei:

- Támogatja a szervezet kockázatelemzését, és a kockázatok figyelembevételével történő döntéshozatalt.
- Fokozza az információbiztonsági tudatosságot, és a szervezet IT és ICS biztonsággal kapcsolatos párbeszédeket is elősegíti.
- Rámutat a rendszerek sérülékenységeire és ajánlást nyújt a biztonsági rések befoltozására.
- Megmutatja a szervezet jó gyakorlatait, és rávilágít az erősségekre.
- Módszert biztosít a kiberrendszerek megfelelésének és monitorozásának tökéletesítésére.
- Átfogóan értékeli a szervezet kiberrendszereit.

A CSET a GitHub-ról letölthető a következő linken:

https://github.com/cisagov/cset/releases

Az eszközről részletesebb tájékoztatás elérhető a következő linkeken:

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

https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf

ICS képzések, oktatások

A teljesség igénye nélkül 2020. júniusban, ICS biztonság tárgyában a COVID-19 világjárványra tekintettel a SANS kizárólag online formában tart ICS képzéseket és oktatásokat.

A képzések részletei a következő webhelyen érhetők el:

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 videóalapú 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, amelynek keretében 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 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 tanfolyamokat egyedi igényeknek megfelelően 0-3 vagy 4-12 hónap időtávban van lehetőség elvégezni. 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 megtartásra.

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. júniusban 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.

Industrial Control Systems (ICS) Cyber Security Conference

A SecurityWeek ICS kiberbiztonsági konferenciáján a résztvevők megismerkedhetnek a legújabb ICS biztonsági incidensekkel, azok elemzéseiben is részt vehetnek, illetve a megoldások kutatásában egyaránt.

Industrial Control Systems (ICS) Cyber Security Conference; (Singapore – virtuális), 2020. június 16-18.

További információk a következő linken találhatók:

https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

CS4CA WORLD: Global Cyber Security Conference

A virtuális konferencia áttekinti a klasszikus IT vs. OT problémákat, valamint a kritikus elemek védelmének előtérbe helyezésével a folyamatok biztonságát is érinti. A kritikus elemek biztonságos protokolljai is érintve lesznek az online térben megrendezett konferencián.

CS4CA WORLD: Global Cyber Security Conference; Virtuális, 2020. június 30.

További információk a következő linken találhatók:

https://world.cs4ca.com/

ICS incidensek

Izrael tájékoztatása: hekkerek támadják a vízágazat SCADA rendszereit

Az izraeli Nemzeti Kibervédelmi Igazgatóság jelentése szerint támadók célba vették a szennyvíztisztító létesítmények SCADA rendszereit.

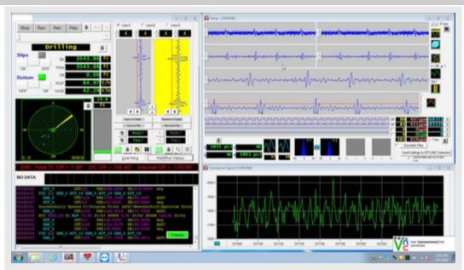
A Kibervédelmi Igazgatóság felhívta a víz- és energia ágazati szereplők figyelmét, hogy az internet felől elérhető felügyeleti rendszerek jelszavait haladéktalanul cseréljék le, valamint a vezérlő- és felügyeleti rendszer szoftverek legyenek frissítve.

A tájékoztatás szerint az egész országban észlelték a támadásokat, de az Izraeli Vízügyi Hatóság szerint az üzemeltetésben nem okoztak fennakadásokat a támadások. A Hatóság kérése szerint az incidenseket jelenteni kell az érintetteknek.

Az incidensről kiadott frissített tájékoztatóban elhangzott, hogy nemcsak a SCADA rendszereket, hanem a teljes ICS rendszereket támadták. A SecurityWeek forrásai szerint a támadók a szelepek vezérlésére használt programozható logikai vezérlőket (PLC-ket) célozták meg a támadás során. A PLC-ben végrehajtott módosítások valóban megtörténtek, ebből arra lehet következtetni, hogy a támadók pontosan tudták, hogy mit csinálnak. Az viszont nem világos, hogy a végső cél volt a szelepek vezérlése, vagy a PLC módosításokkal nyomot hagytak maguk után a támadók.

A Radiflow izraeli kiberbiztonsági cég közzétette, hogy gyakran mobil- vagy rádió telefonos kommunikációval valósítják meg a rendszerek távoli elérését. Mivel a routerek a kommunikáció ezen módja miatt fokozottan vannak kitéve támadásoknak, így ezt próbálták meg kihasználni a szóban forgó támadók is. A másik lehetőség a kiberbiztonsági cég szerint, hogy az ellátási láncokban eredő lehetőségeket kihasználva valósultak meg a támadások, vagyis a legálisan hozzáféréssel rendelkező szervezetek megtámadása után, a hozzáféréseket kihasználva történtek azok.

Mivel a megtámadott szennyvíztisztítók nem kezelnek bizalmas információkat, valószínűsíthető, hogy a károkozás volt a támadók célja. A SCADAfence IT és OT biztonsággal foglalkozó cég szerint a kibertámadásokat a gázai övezetből indította egy Izrael-ellenes hacktivista csoport. A kiberbiztonsági cég azt is elmondta, hogy további támadásokra lehet számítani, és nem csak a vízágazatban.



További részleteket a következő webhelyeken ismerhet meg:

https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities?

https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources?

Könyvajánló

A **Handbook of SCADA/Control Systems Security** könyv az ipari irányító rendszerek és a SCADA rendszerek alapvető biztonsági kérdéseit tárgyalja, különböző, a témában illetékes szakértők szemszögéből. A kiadvány számos fotóval, adattal és illusztrációval igyekszik érthetőbbé és élvezetessé tenni az olvasói számára a SCADA/ICS biztonságot.

A hat fejezetből álló könyv bemutatja a SCADA/ICS rendszerek társadalomra gyakorolt hatásait és a használat következményeit, a szabályozási és menedzsment kérdéseket, az említett rendszerek architektúráit és modelljeit, az üzembe helyezés és üzemeltetés kérdéseit, valamint a SCADA/ICE rendszerek jövőbeli biztonsági tényezőit.

Különböző kiberbiztonsági és a SCADA/ICS rendszerek biztonságával kapcsolatos esettanulmányokat is bemutatnak a szerzők.

A könyv számos jó gyakorlattal szolgál az üzleti környezet biztonsága, stratégiai és technikai kérdések terén, továbbá remekül illeszthetők a leírtak a kritikus infrastruktúra védelmi programokba.

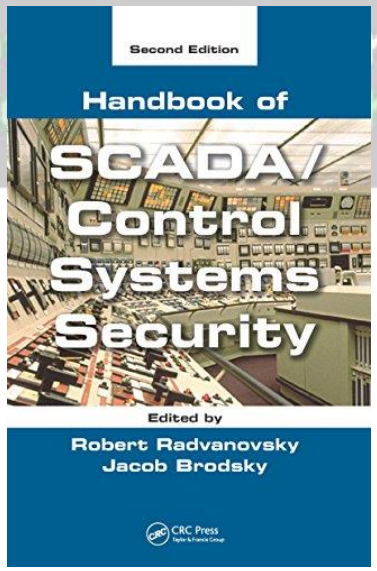
A könyv címe: **Handbook of SCADA/Control Systems Security**

Szerzők: Robert Radvanovsky, Jacob Brodsky

Kiadás éve: 2016.

A kiadvány elérhető a következő linken:

https://www.amazon.co.uk/Handbook-SCADA-Control-Systems-Security-ebook/dp/B01EUQGFGM/ref=sr_1_1?creativeASIN=B01EUQGFGM&dchild=1&imprToken=LM2ftYPP4JaX.CLszMQD-A&keywords=Handbook+of+SCADA%2FControl+Systems+Security&linkCode=g13&qid=1588576752&sr=8-1



Black Cell javaslatok

Az ipari irányító rendszerek biztonságával kapcsolatban rengeteg információ, vélemény, cikk, tanulmány elérhető az interneten. Számos IT és információbiztonsággal foglalkozó weboldal létezik, amely publikál az ICS/SCADA biztonsággal kapcsolatban. Aki pontosan tudja, hogy hol is kell ezeket az írásokat keresni, az hatékonyabban, időt spórolva megtalálja az újdonságokat.

A következő felsorolás segítséget kíván nyújtani azon szervezeteknek, illetve azon személyeknek, akik OT üzemeltetéssel és/vagy biztonsággal foglalkoznak, és a sérülékenységmenedzsmenthez vagy egyáltalán az ICS/SCADA biztonság megteremtéséhez megfelelő információhoz jusson, valamint az újdonságokkal, trendekkel, támadási technikákkal és incidensekkel is megismerkedhessen.

https://www.securityweek.com/scada-ics

https://securityaffairs.co/wordpress/category/ics-scada

https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

https://iiot-world.com/cybersecurity/

https://www.cipsec.eu/content/icsscada-networks-threats-and-defenses

https://industrialcyber.co/

https://www.scadahacker.com/

https://icscybersec.blog.hu/tags/SCADA

https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

https://www.criticalinfrastructureprotectionreview.com/

https://ics.sans.org/ics-library/helpful-websites

https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity

https://www.cirint.eu/

A lista nem teljeskörű, további hasznos weboldalak találhatók, amennyiben megfelelő keresési technikát alkalmazunk.

ICS sérülékenységek

2020. májusában 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-20-147-01: **Inductive Automation Ignition**

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

ICSA-20-147-02: **Johnson Controls Kantech EntraPass**

Magas szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-147-02

ICSA-20-142-01: **Johnson Controls Software House C-CURE 9000 and American Dynamics victor VMS**

Kritikus szintű sérülékenység: szenzitív információk szabad szöveges formában történő tárolása.
https://www.us-cert.gov/ics/advisories/icsa-20-142-01

ICSA-20-142-02: **Schneider Electric EcoStruxure Operator Terminal Expert**

Magas szintű sérülékenységek: SQL és argumentum befecskendezés, útvonal bejárás.
https://www.us-cert.gov/ics/advisories/icsa-20-142-02

ICSA-20-140-02: **Emerson OpenEnterprise**

Kritikus szintű sérülékenységek: kritikus funkció hiányzó hitelesítése, nem megfelelő tulajdonosi menedzsment, nem megfelelő erősségű titkosítás.
https://www.us-cert.gov/ics/advisories/icsa-20-140-02

ICSA-20-140-01: **Rockwell Automation EDS Subsystem**

Magas szintű sérülékenységek: memória puffer határain belüli műveletek nem megfelelő korlátozása, SQL befecskendezés.
https://www.us-cert.gov/ics/advisories/icsa-20-140-01

ICSA-20-135-01: **Opto 22 SoftPAC Project**

Kritikus szintű sérülékenységek: a fájlnév vagy elérési út külső kontrollja, kriptográfiai aláírás hibás ellenőrzése, nem megfelelő hozzáférés ellenőrzés, ellenőrizetlen elem a keresési útvonalban, nem megfelelő engedélyezés.
https://www.us-cert.gov/ics/advisories/icsa-20-135-01

ICSA-20-135-02: **Emerson WirelessHART Gateway**

Kritikus szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-135-02

ICSA-19-213-04: **3S-Smart Software Solutions GmbH CODESYS V3 (Update A)**

Magas szintű sérülékenység: nem megfelelően védett hitelesítő adatok.
https://www.us-cert.gov/ics/advisories/icsa-19-213-04

ICSA-20-133-01: Eaton Intelligent Power Manager

Magas szintű sérülékenységek: nem megfelelő bemeneti hitelesítés, helytelen privilégium kezelés.
https://www.us-cert.gov/ics/advisories/icsa-20-133-01

ICSA-20-133-02: OSIsoft PI System

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

ICSA-20-105-05: Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update A)

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás, nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-105-05

ICSA-20-105-08: Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update A)

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

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

Magas szintű sérülékenység: puffer nem megfelelő méretezése.
https://www.us-cert.gov/ics/advisories/icsa-20-042-06

ICSA-19-274-01: Interpeak IPnet TCP/IP Stack (Update D)

Kritikus szintű sérülékenységek: puffer túlcsordulás, érték-kezelési hiba, memória pufferen belüli műveletek nem megfelelő korlátozása, argumentum befecskendezés, null pointer dereferencia, nem megfelelő szinkronizáció.
https://www.us-cert.gov/ics/advisories/icsa-19-274-01

ICSA-19-255-02: 3S-Smart Software Solutions GmbH CODESYS V3 Library Manager (Update A)

Magas szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-19-255-02

ICSA-19-227-04: Siemens SINAMICS (Update C)

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-227-04

ICSA-19-190-05: Siemens SIPROTEC 5 and DIGSI 5 (Update C)

Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-190-05

ICSA-20-128-01: Advantech WebAccess Node

Kritikus szintű sérülékenységek: nem megfelelő index hitelesítés, útvonal bejárás, puffer túlcsordulás, memória pufferen kívüli olvasás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-20-128-01

ICSA-20-126-01: Fazecast jSerialComm

Magas szintű sérülékenység: ellenőrizetlen keresési útvonal.
https://www.us-cert.gov/ics/advisories/ICSA2012601

ICSA-20-126-02: SAE IT-systems FW-50 Remote Telemetry Unit (RTU)

Kritikus szintű sérülékenységek: XSS, útvonal bejárás.
https://www.us-cert.gov/ics/advisories/ICSA2012602

ICSA-20-119-01: LCDS LAquis SCADA

Közepes szintű sérülékenységek: érzékeny adatok feltárása, nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-119-01

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. május 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