20. 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:

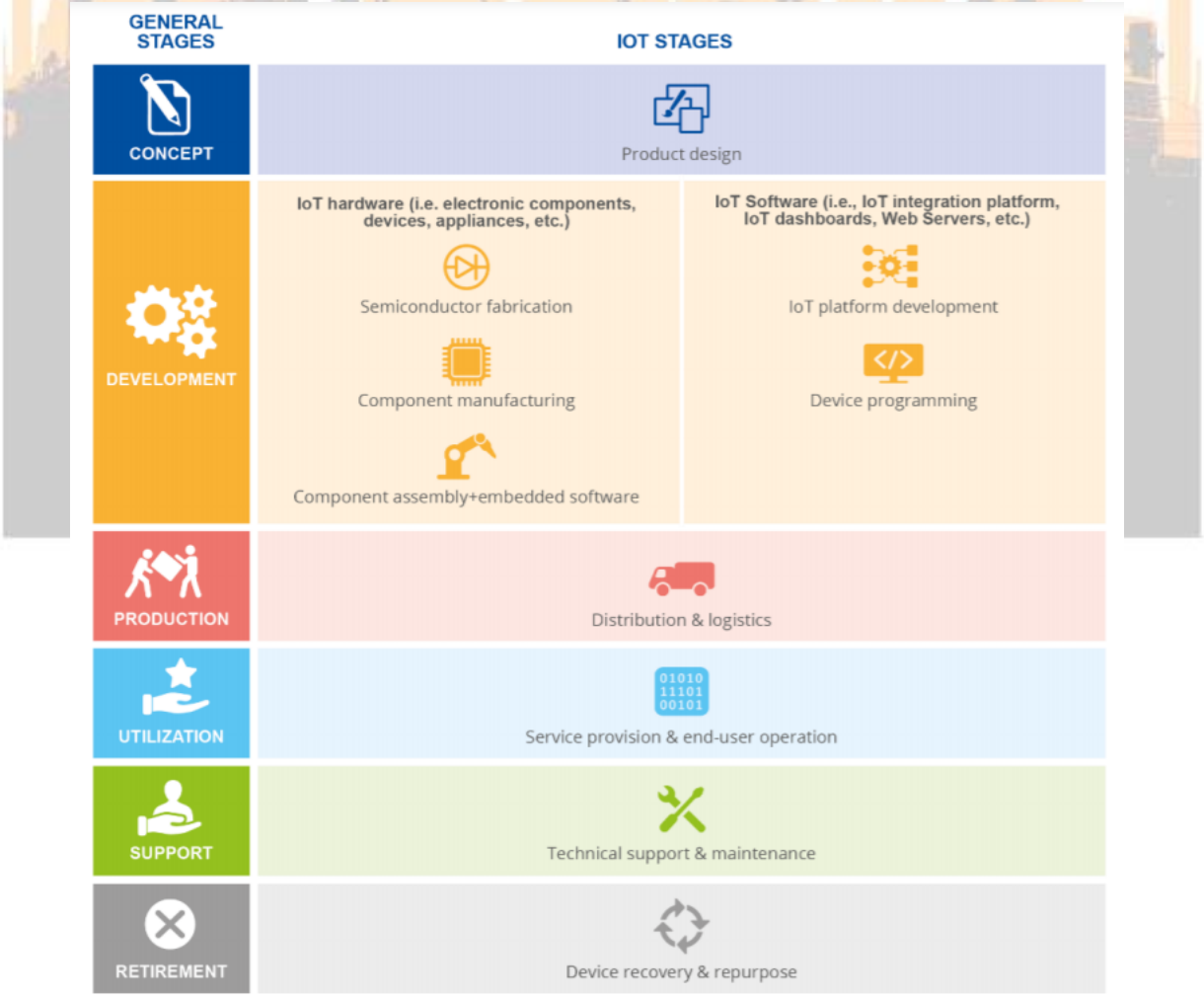
ICS jó gyakorlatok, javaslatok

Az ENISA (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) november 20-án publikált egy útmutatót, amely a dolgok internete (Internet of Things – IoT) ellátási láncában rejlő veszélyek elleni biztonságot hivatott elősegíteni különböző szervezeteknél, amelyek az ellátási lánc résztvevői. Az útmutató a következő linken érhető el:

https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

Az IoT ellátási lánc az alábbi szakaszokból épül fel:

- termék tervezés,
- félvezető gyártás,
- komponens gyártás,
- IoT platform fejlesztése,
- komponensek összeállítása, szoftver beágyazása,
- eszköz programozás,
- elosztás, logisztika,
- szolgáltatásnyújtás és végfelhasználói üzemeltetés,
- műszaki támogatás és karbantartás,
- eszköz helyreállítása és újra-felhasználása.



Az útmutató bemutatja az IoT világ ellátási lánccal kapcsolatos tudnivalóit és betekintést enged a fenyegetések taxonómiájának világába. Az IoT eszközökkel kapcsolatos potenciális támadási szcenáriók is bemutatásra kerülnek.

A dokumentumban bemutatott ellátási lánc biztonságának szavatolásához a szerzők jó gyakorlatokat mutatnak be, amelyek alkalmazása ajánlott, hogy mérni tudjuk és fejleszteni a kapcsolódó biztonsági kontrollokat.

Az ellátási lánc szakaszaiban a következő biztonsági tényezők megfontolása javasolt:

1. Termék tervezés: fenyegetettségi modell, naprakész kriptográfiai és szoftver megoldások, szabotázs elleni védelem, fizikai-logikai konvergencia, helyreállítási terv, kombinált biztonsági kontrollok (hardver, szoftver), bizalmi láncok meghatározása, erőforrás korlátok.
2. Félvezető gyártás: hardver biztonsági mechanizmusok, hulladék menedzsment.
3. Komponens gyártás: hamis - utánzat komponensek, hibás alkatrészek.
4. IoT platform fejlesztése: firmware hozzáférési kontrollok, hátsó kapuk (backdoors).
5. Komponensek összeállítása, szoftver beágyazása: biztonságos kiépítés, kódolási gyakorlat.
6. Eszköz programozás: kockázat alapú fejlesztés, függőség menedzsment, hálózati biztonság, menedzsment támogatás, kényelmi kompromisszumok, üzemeltetők általi használat, biztonsági megoldások implementálása, technikai támogatás, hozzáférés kontroll.
7. Elosztás, logisztika: VAR – hozzáadott értékkel növelt tovább-értékesítés, lopás elleni védelem és hamisítványok, eszköz és regisztrációja nyomon követhetőségének biztosítása.
8. Szolgáltatásnyújtás és végfelhasználói üzemeltetés: Over-The-Air kontroll eszközök, patch menedzsment.
9. Eszköz helyreállítása és újra-felhasználása: adatok eltávolítása.

Napjainkban egyre nagyobb gondot jelentenek az ellátási láncokban rejlő fenyegetések, a világjárvány következtében. Az útmutató aktuális kérdésekre ad választ. Javasolt a dokumentum áttanulmányozása, és az ellátási láncban elfoglalt szerepnek megfelelően értékelni a fenyegetéseket, és a javaslatokat implementálni, melyeket az ENISA ajánl az olvasók számára.

ICS képzések, oktatások

A COVID-19 világjárványra tekintettel 2021. januárban 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
  - 2021.01.11-16.
  - 2021.01.18-23.
  - 2021.01.25-30.

- ICS515: ICS Active Defense and Incident Response
  - 2021.01.11-15.
  - 2021.01.25-29.

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

International Conference on Advanced Industrial Control Technology

A 15. alkalommal megrendezésre kerülő fejlett ipari technológiákról szóló konferencián a témában tevékenykedő tudósok és kutatók osztják meg egymással az elmúlt egy év során elért legfrissebb eredményeket.

A témát érintő legújabb innovációk, trendek is bemutatásra kerülnek a résztvevők számára, ahogy a kihívások is, melyekkel meg kell küzdeni a különböző ipari technológiákat alkalmazó, fejlesztő, tervező, üzemeltető szereplőknek.

ICAICT 2021: 15. International Conference on Advanced Industrial Control Technology; (Szingapúr, Szingapúr), 2021.01.11 – 2021.01.12.

További információk a következő linken találhatók:

https://waset.org/advanced-industrial-control-technology-conference-in-january-2021-in-singapore

Cyber Security for Critical Assets APAC Summit

A konferencián a koronavírus okozta fenyegetések bemutatásra kerülnek a résztvevők számára. Az otthoni munkavégzés sajátosságaiból fakadó IT és OT üzemeltetés kockázatai is részleteiben megismerhetők lesznek, és az összkockázat szemszögéből a kritikus infrastruktúrák védelmi rendszere is értékelésre kerül az előadók által.

A konferencia előadói a való életből vett esettanulmányokat is bemutatnak, továbbá rendkívül érdekesnek ígérkezik a MITRE ATT&CK keretrendszer szervezeti fejlesztési lehetőségeiről szóló előadás. Az IT és OT fizikai biztonság közötti különbségeket is megismerhetik a résztvevők, ahogy a bizalom nélküli (zero trust) OT hálózati stratégiát is.

Cyber Security for Critical Assets APAC Summit; (Virtuális konferencia); 2021.01.27 – 2021.01.28.

További információk a következő linken találhatók:

https://apac.cs4ca.com/

ICS üzemeltetői incidensek

Repülőgépgyártó vált zsarolóvírus áldozatává

Az Embraer egy brazíliai légi közlekedési eszközöket gyártó cég, amely weblapja információi szerint a 3. legnagyobb repülőgépgyártó a világon, és utasszállító, katonai, valamint mezőgazdasági repülők gyártásával foglalkozik.

A vállalat sajtóközleményt adott ki, mely szerint november végén a szervezet IT rendszerét kibertámadás érte. Azóta is kevés információ látott napvilágot, melyet a szervezet megosztott a nyilvánossággal, ebben megemlítve, hogy kizárólag egyetlen logikai helyen tárolt fájlok elérhetetlenségét okozta a támadás.

A cég a közleményében kifejtette, hogy a rendelkezésre álló eljárásrendek mentén elkezdődött az eseménykezelés, amelyek átmeneti zavarokat okoztak egyes műveletekben, mert azokat el kellett szigetelni a többi rendszertől.

A készenléti (alternatív) rendszerek segítenek az üzemeltetés fenntartásában, mely működőképes ezen megoldással is. A szervezet mindent elkövet annak érdekében, hogy kivizsgálja a támadás minden egyes részletét. A vizsgálat kiterjed a hatások vizsgálatára, valamint az érintettek beazonosítására (harmadik felek).

Egy brazil hírcsatorna megtudta, hogy egy zsarolóvírus okozta a problémát, amely megzavarta az otthonról dolgozók hozzáféréseit a rendszerekhez.

A cég további információt nem osztott meg az érdeklődőkkel.

A támadással kapcsolatos információk a következő linken érhetők el:

https://www.securityweek.com/brazilian-plane-maker-embraer-targeted-cyberattack

Szerző: Az incidensről kiderült információk elég szegényesek, azonban az megállapítható, hogy napjaink egyik legnagyobb fenyegetése a ransomware támadás. Könnyen véghezvihető és nagy károkat tud okozni egy zsarolóvírus támadás. Az ipari vezérlő rendszerek is gyaníthatóan érintettek voltak a támadásban, ha nem is közvetlenül, de az események kezelése során rendszer szegmentációra kényszerült a szervezet, ezáltal a távoli hozzáférésekkel is gond keletkezett. Kérdés, hogy ezt a problémát maga a zsarolóvírus támadás okozta, vagy az incidenskezelési lépések? Ha az incidenskezelési lépések, akkor nagy valószínűséggel az üzletmenet-folytonossági tervek nem megfelelően működtek, ha a zsarolóvírus okozta, akkor pedig nem volt megfelelő preventív védelem kialakítva a szervezet tekintetében. Javasoljuk a ransomware kockázatokat minden szervezetnél elemezni és a kockázatokkal arányos védelmi intézkedéseket implementálni!

Könyvajánló

Joseph Weiss az ipari irányító rendszerek elektronikus fenyegetésekkel szembeni védelmét mutatja be a könyvben. Az olvasó pontos magyarázatot kap az IT (Information Technology) és az OT (Operational Technology) különbségeiről, továbbá az ipari irányító rendszerek elektronikus fenyegetéseiről. A könyv 2010-ben íródott, így a szakavatott szemek az elmúlt 10 évben történt változásokat is képesek megállapítani és ez rávilágíthat arra, milyen gyorsan változik az ipari rendszerek kiberbiztonsági rendszere.

Az ipari irányító rendszerek összetett biztonsági megközelítése szerinti 3 alkotóelemet is részletesen megismerheti az olvasó, melyek a következők: ICS biztonság, IT biztonság, fizikai biztonság.

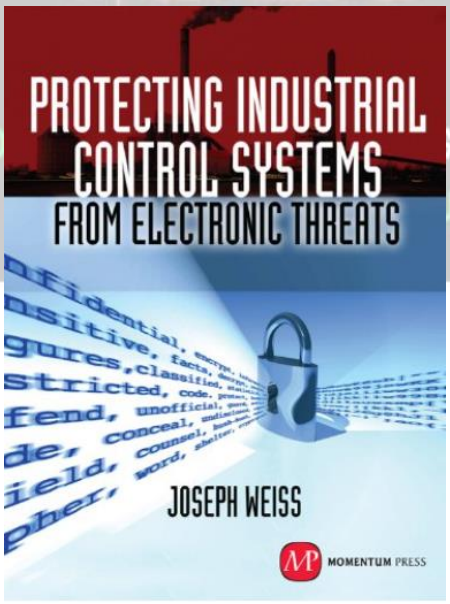
A könyvben szó esik az információmegosztás fontosságáról, valamint a kiber fenyegetések kockázatainak értékeléséről is. A szándékos támadások mellett a nem szándékos cselekmények során bekövetkező incidensek is bemutatásra kerülnek. Az ipari irányító rendszereket érő incidensek kategorizálását is megismerheti az olvasó, továbbá ajánlásokat is megfogalmaz a szerző a kiberbiztonság fokozása érdekében.

A könyv címe: Protecting Industrial Control Systems from electronic threats

Szerzők/szerkesztők: Joseph Weiss

Kiadás éve: 2010.

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



Black Cell javaslatok

A SCADA hálózatok kiberbiztonságának fejlesztése

Az Egyesült Államok Energiaügyi Minisztériuma és a Kritikus Infrastruktúra Védelmi Szervezete még a kétezres évek elején kiadott egy 21 lépésből álló útmutatót, amely segítséget nyújt a SCADA hálózatok kiberbiztonságának fejlesztéséhez. A dokumentum régisége ne tévesszen meg senkit, a mai napig aktuális jó gyakorlatok kerülnek benne megfogalmazásra. A 21 lépés, melyek részleteiben is kifejtésre kerülnek a dokumentumban, a következők:

1. Azonosítsuk a SCADA rendszerünk összes kapcsolódási/kapcsolati pontját.
2. Szüntessük meg a szükségtelen kapcsolatokat.
3. Értékelje és szükség esetén erősítse meg a fennmaradó SCADA kapcsolatok biztonságát.
4. Végezzen „hardening" tevékenységet a SCADA hálózatok felesleges szolgáltatásainak eltávolításával vagy letiltásával.
5. Vizsgálja meg a protokollok biztonságát, amely a rendszerben használatban van.
6. Az eszköz és szolgáltatás vendorok által nyújtott biztonsági szolgáltatásokat használja ki, és végezze el a biztonsági beállításokat.
7. A SCADA hálózathoz csatlakoztatható adathordozók felett alakítson ki megfelelő kontrollokat.
8. Implementáljon külső és belső behatolás érzékelő rendszereket (IDS – Intrusion Detection System), és biztosítsa a 24 órás figyelemmel kísérését az eseményeknek.
9. Végezzen technikai auditot a SCADA eszközökön és hálózatokon, valamint minden más csatlakoztatott eszközön - hálózaton, a biztonsági problémák azonosítása érdekében.
10. Felmérésekkel értékelje a fizikai biztonságot, a távoli hálózati kapcsolatok tekintetében is.
11. Hozzon létre SCADA „Red Team" csoportot a lehetséges támadási forgatókönyvek azonosításához és értékeléséhez.
12. Az érintettek számára világosan határozza meg a kiberbiztonsági szerepeket, felelősségeket és jogosultságokat a vezetők, rendszergazdák és felhasználók számára.
13. Dokumentálja a hálózati architektúrát és azonosítsa a kritikus funkciókat kiszolgáló rendszereket, amelyek további védelmet, magasabb védelmi szintet igényelnek.
14. Alakítson ki megfelelő szintű kockázatmenedzsment rendszert.
15. Hozzon létre egy hálózati védelmi stratégiát a mélységi védelem (Defense-In-Depth) elve alapján.
16. Világosan határozza meg a kiberbiztonsági elvárásokat.
17. Alakítson ki hatékony konfiguráció menedzsment folyamatokat.
18. Rutinszerűen végezzen rendszeresen önértékelést.
19. Gondoskodjon a SCADA hálózatban található adatok mentéséről, és alakítson ki megfelelő szintű katasztrófa helyreállítási terveket (Disaster Recovery Plan – DRP)
20. A szervezet vezetői a világos kiberbiztonsági elvárások figyelembevétele mellett alakítsa ki a felelősségre vonás rendszerét.
21. Hozzon létre szervezeti szabályozókat, melyek tartalmát és folyamatainak működőképességét oktatással biztosítsa a szervezet munkavállalói és a további érintettek részére, ellenőrizze a hatékonyságot.

A dokumentum megtalálható a következő linken:

https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

ICS sérülékenységek

2020. decemberében 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-20-352-02: **PTC Kepware KEPServerEX** (Update A)
Kritikus szintű sérülékenységek: puffer túlcsordulás, memória felszabadítási hibák.
https://us-cert.cisa.gov/ics/advisories/icsa-20-352-02

ICSA-20-308-03: **ARC Informatique PcVue** (Update A)
Kritikus szintű sérülékenységek: nem megbízható adatok kezelése, kritikus magánváltozóhoz történő nyilvános hozzáférés, érzékeny információk feltárása jogosulatlanok számára.
https://us-cert.cisa.gov/ics/advisories/icsa-20-308-03

ICSA-20-282-01: **Johnson Controls Sensormatic Electronics American Dynamics victor Web Client and Software House C CURE Web Client** (Update A)
Magas szintű sérülékenység: nem megfelelő engedélyezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-01

ICSA-20-224-01: **Yokogawa CENTUM** (Update A)
Magas szintű sérülékenységek: nem megfelelő hitelesítés, útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-01

ICSA-20-212-02: **Mitsubishi Electric Multiple Factory Automation Engineering Software Products** (Update A)
Magas szintű sérülékenység: engedélyezési hibák.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-02

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

ICSA-20-352-01: **Emerson Rosemount X-STREAM**
Magas szintű sérülékenység: nem megfelelő hitelesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-352-01

ICSA-20-352-02: **PTC Kepware KEPServerEX**
Kritikus szintű sérülékenységek: puffer túlcsordulás, memória felszabadítása utáni nem várt értékhasználat vagy kód futtatás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-352-02

ICSA-20-352-03: **PTC Kepware LinkMaster**
Kritikus szintű sérülékenység: helytelen alapértelmezett engedélyek.
https://us-cert.cisa.gov/ics/advisories/icsa-20-352-03

ICSA-20-308-01: WAGO Series 750-88x and 750-352 (Update A)

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.

https://us-cert.cisa.gov/ics/advisories/icsa-20-308-01

ICSMA-20-345-01: Medtronic MyCareLink Smart

Magas szintű sérülékenységek: nem megfelelő hitelesítés, puffer túlcsordulás, nem megbízható adatok ellenőrzés nélküli elvetése.

https://us-cert.cisa.gov/ics/advisories/icsma-20-345-01

ICSA-20-345-01: Mitsubishi Electric MELSEC iQ-F Series

Magas szintű sérülékenység: kivétel kondíciók kezelésének nem megfelelő ellenőrzése.

https://us-cert.cisa.gov/ics/advisories/icsa-20-345-01

ICSA-20-345-02: Host Engineering H2-ECOM100 Module

Magas szintű sérülékenység: nem megfelelő bemeneti érvényesítés.

https://us-cert.cisa.gov/ics/advisories/icsa-20-345-02

ICSMA-20-343-01: GE Healthcare Imaging and Ultrasound Products

Kritikus szintű sérülékenységek: hitelesítő adatok védtelen továbbítása, érzékeny rendszerinformációk kitettsége jogosulatlanok számára.

https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01

ICSA-20-343-01: Multiple Embedded TCP/IP Stacks

Kritikus szintű sérülékenységek: elérhetetlen kilépési kondíciók, egész szám túlcsordulás, memória puffer határain kívüli olvasás és írás lehetősége, nem megfelelő bemeneti érvényesítés, nem megfelelő null érték kezelés.

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

ICSA-20-343-02: Mitsubishi Electric GOT and Tension Controller

Magas szintű sérülékenység: memória puffer határain kívüli olvasás lehetősége.

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-02

ICSA-20-343-03: Schneider Electric Easergy T300

Kritikus szintű sérülékenységek: kritikus funkció hiányzó autentikációja, hiányzó engedélyezés, érzékeny információk hiányzó titkosítása, felhasználói felület rétegeinek nem megfelelő korlátozása.

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-03

ICSA-20-343-04: Schneider Electric Modicon M221 Programmable Logic Controller

Magas szintű sérülékenységek: nem megfelelő erősségű titkosítás, véletlenszerű értékek nem megfelelő méretezésű logikai helye, érzékeny információk hiányzó titkosítása, érzékeny információk feltárása, egyirányú hash használata kiszámítható sózással.

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-04

ICSA-20-343-05: Siemens Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33)

Közepes szintű sérülékenység: egész szám túlcsordulás.

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

ICSA-20-343-06: Siemens XHQ Operations Intelligence
Magas szintű sérülékenység: érzékeny információk jogosulatlanok számára történő feltárása, XSS, SQL befecskendezés, útvonal bejárás, CSRF.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-06

ICSA-20-343-07: Siemens SICAM A8000 RTUs
Magas szintű sérülékenység: védelmi mechanizmus hiba.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-07

ICSA-20-343-08: Siemens Products using TightVNC
Kritikus szintű sérülékenységek: puffer túlcsordulás, null pointer dereferencia.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-08

ICSA-20-343-09: Siemens SIMATIC Controller Web Servers
Közepes szintű sérülékenység: nem megfelelő kivétel kezelés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-09

ICSA-20-343-10: Siemens LOGO! 8 BM
Kritikus szintű sérülékenységek: kritikus funkció hiányzó autentikációja, beégetett kriptográfiai kulcs használata, kockázatos kriptográfiai algoritmus használata, nem megfelelően védett hitelesítési adatok.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-10

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

ICSA-20-252-07: Siemens Industrial Products (Update B)
Közepes szintű sérülékenység: érzékeny információk jogosulatlanok számára történő feltárása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

ICSA-20-224-05: Siemens SIMATIC, SIMOTICS (Update A)
Alacsony szintű sérülékenység: erőforrás állapot változás ellenőrzési hiba.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-05

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

ICSA-20-161-03: Siemens LOGO! (Update A)
Kritikus szintű sérülékenység: kritikus funkció hiányzó autentikációja.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-03

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update D)
Közepes szintű sérülékenység: ellenőrizetlen elem a keresési útvonalban.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

ICSA-20-161-05: Siemens SIMATIC, SINAMICS (Update B)
Magas szintű sérülékenységek: ellenőrizetlen elem a keresési útvonalban, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-05

ICSA-20-042-04: Siemens PROFINET-IO Stack (Update C)
Magas szintű sérülékenységek: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04

ICSA-19-253-03: Siemens Industrial Products (Update K)
Magas szintű sérülékenységek: túlzott adat-lekérdezési műveletek, egész szám túlcsordulás, ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03

ICSA-19-134-03: Siemens LOGO! Soft Comfort (Update A)
Magas szintű sérülékenység: nem megbízható adatok ellenőrzés nélküli elvetése.
https://us-cert.cisa.gov/ics/advisories/ICSA-19-134-03

ICSA-19-134-04: Siemens LOGO! 8 BM (Update A)
Kritikus szintű sérülékenységek: kritikus funkció hiányzó autentikációja, az elvártnál több érték nem megfelelő kezelése, jelszavak egyszerű szöveges formában történő tárolása.
https://us-cert.cisa.gov/ics/advisories/ICSA-19-134-04

ICSA-18-165-01: Siemens SCALANCE X Switches, RUGGEDCOM WiMAX, RFID 181-EIP, and SIMATIC RF182C (Update D)
Magas szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/ICSA-18-165-01

ICSA-17-243-02: Siemens LOGO! (Update A)
Magas szintű sérülékenységek: nem megfelelően védett hitelesítési adatok, közbe-ékelődéses támadásnak kitettség (Man-In-The-Middle)
https://us-cert.cisa.gov/ics/advisories/ICSA-17-243-02

ICSA-20-338-01: National Instruments CompactRIO
Magas szintű sérülékenység: kritikus erőforrás helytelen engedélyezési folyamata.
https://us-cert.cisa.gov/ics/advisories/icsa-20-338-01

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

ICSA-20-203-01: Wibu-Systems CodeMeter (Update D)
Kritikus szintű sérülékenységek: puffer hozzáférés helytelen hosszúságú értékkel, nem megfelelő erősségű titkosítás, eredetellenőrzési hiba, nem megfelelő bemeneti hitelesítés, kriptográfiai aláírás nem megfelelő ellenőrzése, nem megfelelő erőforrás leállítás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

ICSA-20-336-01: Schneider Electric EcoStruxure Operator Terminal Expert runtime (Vijeo XD)
Magas szintű sérülékenység: nem megfelelő privilegizált hozzáférés menedzsment.
https://us-cert.cisa.gov/ics/advisories/icsa-20-336-01

ICSA-20-329-01: Rockwell Automation FactoryTalk Linx
Kritikus szintű sérülékenységek: nem megfelelő bemeneti érvényesítés, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-329-01

ICSA-20-329-02: Fuji Electric V-Server Lite
Magas szintű sérülékenység: memória puffer határain kívüli írás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-20-329-02

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