16. 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.

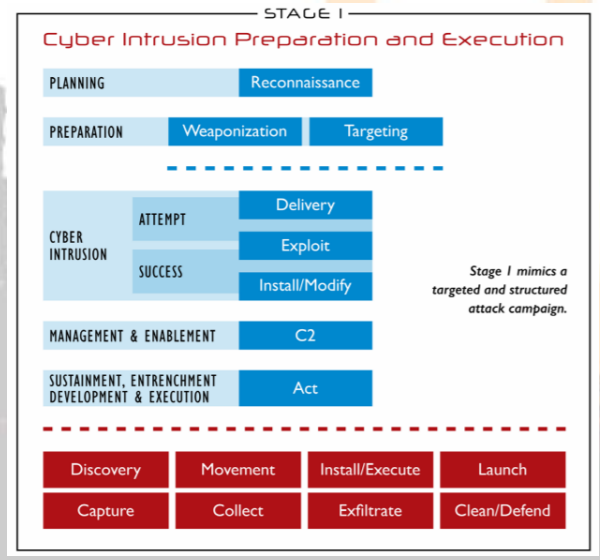
Tartalom:

ICS jó gyakorlatok, javaslatok

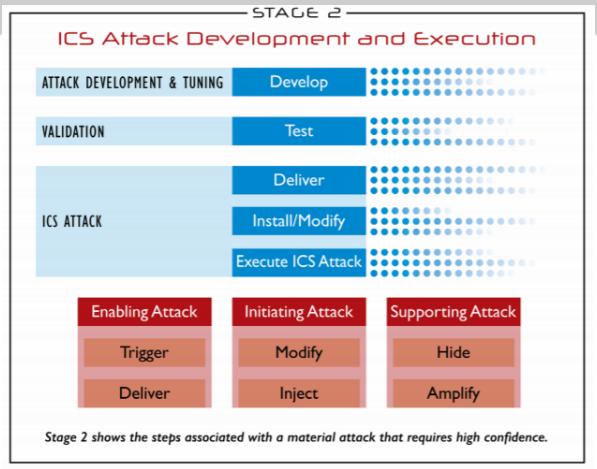
Az ICS rendszerek biztonságát szavatolni kívánó szervezetnek ismernie kell, hogy az adott rendszerek ellen milyen módon követhetnek el támadást bizonyos hacker vagy APT csoportok. Ehhez nélkülözhetetlen az ICS rendszerek elleni támadások menetének (ún. „cyber kill chain") ismerete.

Az ICS cyber kill chain bemutatására a SANS Institute még 2015-ben adott ki egy whitepapert, mely az idei évben frissítésre került. Az egyszerű IT rendszerek elleni támadások cyber kill chain-je különbözik valamelyest az ICS rendszerekétől, többek között a célját és kifinomultságát tekintve.

A SANS által kiadott dokumentum bemutatja az első fázist, amely a kémkedést és információszerzést jelenti, és amely a behatolást készíti elő. Ezt követően a logikai behatolás következik, majd az ICS rendszerben végzett tevékenységek, engedélyek, jogosultságok megszerzése, sérülékenységek kihasználása által.



A C2 (Command & Control) fázisban már a vezérlés a támadónál van sikeres támadás esetén, a kommunikációs csatornák megfelelő kiépítése is megtörténik. A második fázisban a képességek további bővítése zajlik, és az ICS rendszer elleni támadás céljának a megvalósítása.



Az ICS rendszerek elleni támadások céljának és bonyolultságának magyarázatát is tartalmazza a dokumentum, ábrákkal szemléltetve.

A dokumentumban bemutatásra kerül továbbá a HAVEX malware-ről készített esettanulmány, továbbá a Stuxnet cyber kill chain is, és a Purdue modellt is megismerheti az olvasó.

A SANS The Industrial Control System Cyber Kill Chain című whitepaper megtalálható a következő linken:

https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Javasoljuk a dokumentum és az ICS cyber kill chain tanulmányozását annak érdekében, hogy minél inkább megértsük az ICS rendszerek elleni kibertámadások természetét, és fejleszthessük az ellenállóképességét a szervezet OT/IT biztonsági rendszereinek.

ICS képzések, oktatások

A COVID-19 világjárványra tekintettel 2020. szeptemberben 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:

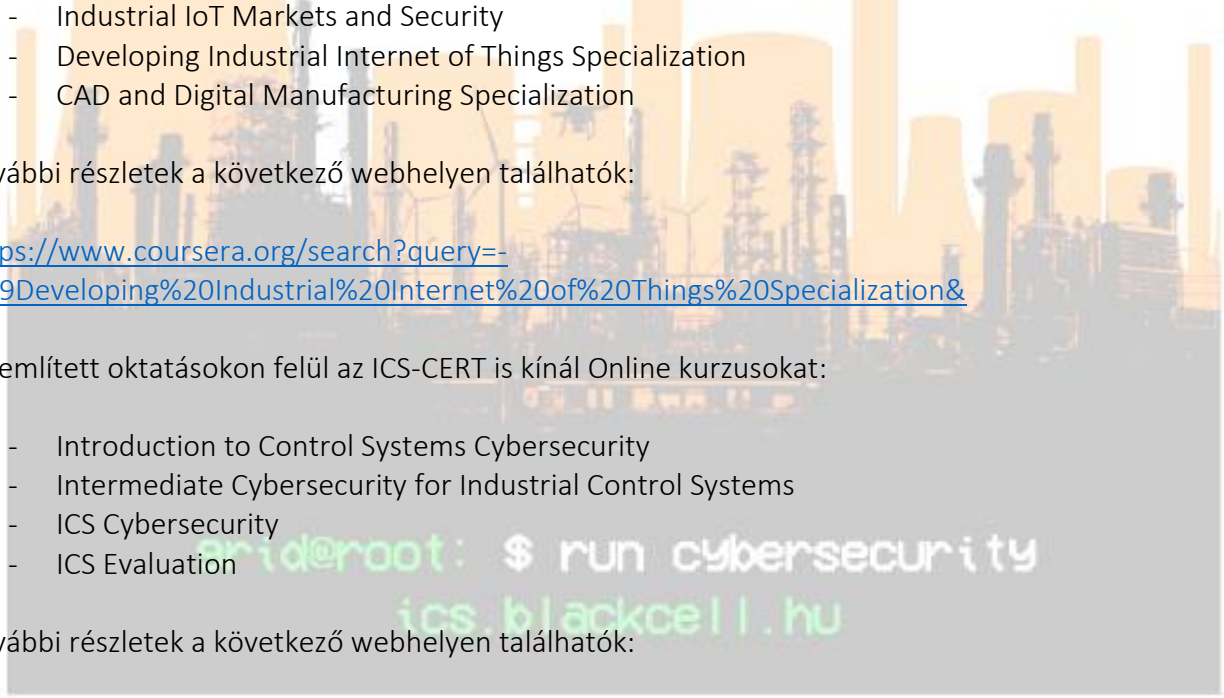
- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization
- CAD and Digital Manufacturing Specialization

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
    - 2020.08.31-09.04.
    - 2020.09.07-11.
    - 2020.09.20-24.

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

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 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 tesztt is.

A képzéssel kapcsolatos további információk a következő linken érhetők el:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

ICS konferenciák

2020. szeptemberében a koronavírus világjárványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop vagy elmarad, vagy valamely későbbi időpontra kerül áthelyezésre. Az alábbi konferenciák azonban virtuálisan vagy a helyszínen biztonsági intézkedések betartása mellett kerülnek megtartásra.

ICS Cyber Security Conference 2020

A NIS irányelvet követő tapasztalatok feldolgozása lesz az egyik témája a konferenciának, ahol a résztvevők megismerhetik az ICS rendszereket védő megoldásokat, azok implementációs lehetőségeit, és a vonatkozó jogszabályi előírásoknak történő megfelelést.

A jelentkezőknek lehetőségük lesz megismerni a témát illetően a jelenlegi piaci megoldásokat és azok megoldásait a biztonság garantálása érdekében. Szó lesz a konferencián a legfrissebb ICS rendszereket érintő kiber- és humán fenyegetésekről is.

ICS Cyber Security Conference 2020; (London, Egyesült Királyság); 2020.08.31-09.03.

További információk a következő linken találhatók:
https://app.qwoted.com/opportunities/event-ics-cyber-security-conference-2020-london

Industrial Cyber Security Summit

A 8. éve megrendezésre kerülő Industrial Cyber Security Summit 2020 konferencián IT és OT biztonsági szakemberektől szerezhetnek be információt a résztvevők a következő témákban: kiberbiztonsági szint mérése és értékelése, ICS rendszerek vállalati rendszerbe történő integrálása, jövőbeli kiberbiztonsági fenyegetések, fejleszteni és fenntartani a vállalati kiberbiztonsági fejlettséget, tudatosságot, a biztonsági kultúrát. A NIST 800-82 keretrendszer használata is bemutatásra kerül a konferencián.

Industrial Cyber Security Summit; (Online konferencia, USA); 2020.09.02-03.

További információk a következő linken találhatók:
https://usa.cs4ca.com/

Kaspersky Industrial Cybersecurity Conference 2020

A Kaspersky által szervezett 8. nemzetközi ICS biztonsági konferencián 40 előadó osztja meg tapasztalatait az ipari irányító rendszerek biztonságával kapcsolatban. A konferencián a világjárványt figyelembe véve a távolságtartás és egyéb egészségügyi intézkedéseket garantálja a szervező.

Kaspersky Industrial Cybersecurity Conference 2020; (Szocsi, Oroszország); 2020.09.02-04.

További információk a következő linken találhatók:
https://ics.kaspersky.com/conference/

ICS incidensek

A GARMIN termelési rendszerében ransomware incidens okozott problémát

Az incidens, amely a GARMIN weboldalát, hálózatát és termelési rendszerét érintette Ázsiában (Taiwan, gyárleállás), ezenkívül a repülési adatbázis szolgáltatások is részesei voltak a zsarolóvírus támadásnak.

A július végén bekövetkezett eseményt a GARMIN hivatalos Twitter-üzenetében is megerősítette és egyben tájékoztatta az ügyfeleket, hogy a kiesés befolyásolta a Call Center működését, illetve ezen ok miatt nem válaszoltak e-mailekre és egyéb csevegőalkalmazásokban az üzenetekre sem.

A GARMIN webszolgáltatása is leállt, amely támogatja a vállalat repülési navigációs berendezéseit is. A ZDnet-nek pilóták is jelezték, hogy nem tudták letölteni a Garmin repülési adatbázisának szükséges verzióját a Garmin repülőgép-navigációs rendszerükre. Ezenkívül a járatok ütemezésére és tervezésére használt Pilot szolgáltatás is kiesett.

Szakértők elmondták, hogy a pontos ransomware-t a rendelkezésre álló információk alapján nem tudták pontosan beazonosítani, azonban azt is megjegyezték, hogy a mai kiberfenyegetési térképen jelenleg a ransomware az a károkozó, amely a legnagyobb hatásfokkal képes bármilyen termelési rendszer tekintetében komoly károkat előidézni, így a gyártósorok leállításával jelentős bevételkiesést okozni. A cég szakértői WastedLocker-nek nevezték a zsarolóvírust.

A cég tájékoztatása alapján a felhasználók adatai nem kerültek veszélybe és nem szivárogtak ki a szervezet rendszereiből, viszont a helyreállítást követően több órán keresztül csak csökkentett üzemmódban tudtak üzemelni a társaság elektronikus információs rendszerei.

A veszteségekről nem közölt adatokat a szervezet, azonban valószínűsíthetően mind a reputációvesztés, mind a jelenlegi gyártáskiesésből származó károk, mind a jövőbeli repülési rendszert érintően jelentkező kártérítési eljárások miatt jelentkező károk meghatározó mértéket fognak ölteni.

Az incidenssel kapcsolatos további információk a következő webhelyeken érhetők el a weboldalakon magyar és angol nyelven egyaránt:

www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack

https://www.hwsw.hu/hirek/62091/garmin-connect-tamadas-ransomware-helyreallitas.html

https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/

https://nki.gov.hu/it-biztonsag/hirek/lehetseges-ransomware-tamadas-a-garminnal/

Könyvajánló

Az ipari irányító rendszerek napjainkban egyre összetettebbek és egyre több rendszerrel kerülnek kapcsolatba a tevékenységek végzésének megkönnyítése érdekében. Régebben megoldható volt a külső rendszerektől történő szeparáció, ez ma már azonban elképzelhetetlen.

A rendszerek komplexitása és összekapcsolása azonban megteremtette a lehetőségét annak, hogy egyre több káros kód és támadási forma veszélyeztesse az ipari irányító rendszereket. A rosszindulatú aktorok számos megoldással próbálkozhatnak, hogy ezen rendszereket kompromittálják.

A Cyber Security for SCADA Systems című könyv elemzi a különféle típusú irányító rendszereket és a hozzájuk kapcsolódó fenyegetéseket, valamint a számítógépes támadások elleni védekezés módszereit.

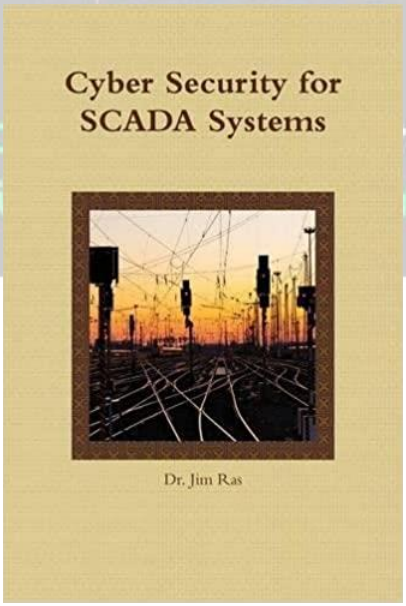
A könyv címe: **Cyber Security for SCADA Systems**

Szerzők/szerkesztők: Dr. Jim Ras

Kiadás éve: 2016.

A kiadvány elérhető a következő linken:

https://www.amazon.co.uk/Cyber-Security-SCADA-Systems-Dr/dp/136551353X/ref=sr_1_2?dchild=1&keywords=Cyber+Security+for+SCADA+Systems&linkCode=gs3&qid=1596201921&sr=8-2&tag=uuid07-21

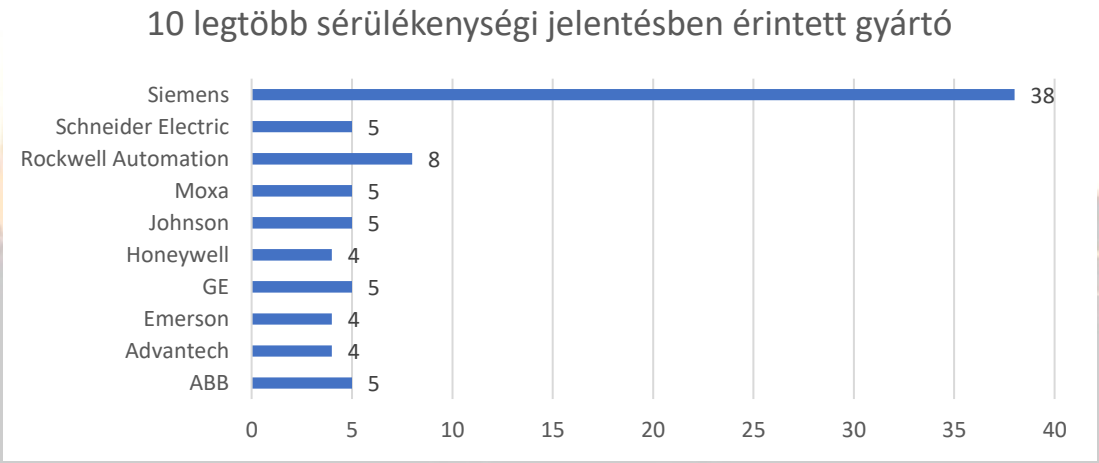


Black Cell javaslatok

Az Egyesült Államok Belbiztonsági Minisztériumának Kiberbiztonsági és Infrastruktúra Biztonsági Ügynöksége (Department of Homeland Security, Cybersecurity & Infrastructure Security Agency) ipari irányító rendszerek biztonságával foglalkozó szervezeti egysége (ICS-CERT) rendszeresen közzéteszi az ICS/SCADA rendszerek és rendszer komponensek sérülékenységeinek jelentéseit, a 2020. augusztusi sérülékenységek is megtalálhatók a következő oldalon.

A Black Cell csapata a 2020. I. félévében publikált sérülékenységeket elemzésnek vetette alá, amely elemzésben megvizsgálta statisztikailag a sérülékenységeket. A Black Cell honlapján publikált sérülékenységi jelentésben megismerheti a letöltő, hogy hány kritikus, magas, közepes és alacsony sérülékenység került publikálásra, mely rendszer sérülékenységi jelentése tartalmazott 54 sérülékenységet, illetve a sérülékenységek mely ágazatokat, alágazatokat érintették a legjobban.

A publikált sérülékenységekben leginkább érintett 10 gyártót az alábbi grafikon mutatja:



A sérülékenység elemzés tartalmazza azt az 5 sérülékenységet, amelyek a leggyakrabban előfordultak az ICS rendszerekben 2020. első félévében.

A sérülékenységek CWE pontok szerinti megoszlását is tartalmazza az elemzés, illetve a publikált sérülékenységekből levonható következtetéseket is.

Az ICS sérülékenységi 2020. első félévi jelentés a következő webhelyről tölthető le:

https://blackcell.hu/ics-serulekenysegi-riport-whitepaper/

ICS sérülékenységek

2020. augusztusában 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-20-240-01: **Red Lion N-Tron 702-W, 702M12-W**

Kritikus szintű sérülékenységek: XSS, CSRF, rejtett funkcionalitás, karbantartás nélküli harmadik fél által üzemeltetett komponens használata.
https://us-cert.cisa.gov/ics/advisories/icsa-20-240-01

ICSMA-20-184-01: **OpenClinic GA (Update A)**

Kritikus szintű sérülékenységek: hitelesítés megkerülése, hitelesítési próbálkozások korlátozásának hiánya, nem megfelelő hitelesítés, hiányzó azonosítás, szükségtelen privilegizált jogosultságok, veszélyes fájltípus korlátozatlan feltöltési lehetősége, útvonal bejárás, nem megfelelő engedélyezés, XSS, karbantartás nélküli harmadik fél által üzemeltetett komponens használata, nem megfelelően védett hitelesítő adatok, rejtett funkcionalitás.
https://us-cert.cisa.gov/ics/advisories/icsma-20-184-01

ICSA-20-238-01: **Advantech iView**

Kritikus szintű sérülékenység: útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-238-01

ICSA-20-238-02: **Emerson OpenEnterprise**

Alacsony szintű sérülékenység: nem megfelelő erősségű titkosítás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-238-02

ICSA-20-238-03: **WECON LeviStudioU**

Magas szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-238-03

ICSMA-20-233-01: **Philips SureSigns VS4**

Közepes szintű sérülékenységek: nem megfelelő bemeneti érvényesítés, nem megfelelő hozzáférés ellenőrzés, nem megfelelő engedélyezés.
https://us-cert.cisa.gov/ics/advisories/icsma-20-233-01

ICSA-20-168-01: **Treck TCP/IP Stack (Update G)**

Kritikus szintű sérülékenységek: Hosszparaméterek nem megfelelő kezelése, nem megfelelő bemeneti érvényesítés, memóriacím duplán történő hívása, memória puffer határain kívüli olvasás lehetősége, nem megfelelő hozzáférés ellenőrzés, egészszám túlcsordulás, nem megfelelő érvénytelenítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

ICSA-20-224-01: **Yokogawa CENTUM**

Magas szintű sérülékenységek: nem megfelelő engedélyezés, útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-01

ICSA-20-224-02: Schneider Electric APC Easy UPS On-Line
Kritikus szintű sérülékenység: útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-02

ICSA-20-224-03: Tridium Niagara
Alacsony szintű sérülékenység: távoli erőforrás szinkron hozzáférés időkorlát nélkül.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-03

ICSA-20-224-04: Siemens SCALANCE, RUGGEDCOM
Kritikus szintű sérülékenység: klasszikus puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-04

ICSA-20-224-05: Siemens SIMATIC, SIMOTICS
Alacsony szintű sérülékenység: erőforrás állapot változás az ellenőrzés és a felhasználás között.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-05

ICSA-20-224-06: Siemens Desigo CC
Kritikus szintű sérülékenység: kód befecskendezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-06

ICSA-20-224-07: Siemens Automation License Manager
Magas szintű sérülékenység: nem megfelelő engedélyezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-07

ICSA-20-224-08: Siemens SICAM A8000 RTUs
Magas szintű sérülékenység: XSS.
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-08

ICSA-20-196-05: Siemens UMC Stack (Update A)
Közepes szintű sérülékenységek: nem jegyzett keresési út vagy elem, ellenőrizetlen erőforrás felhasználás, nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-196-07: Siemens Opcenter Execution Core (Update A)
Magas szintű sérülékenységek: XSS, SQL befecskendezés, nem megfelelő hozzáférés ellenőrzés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-07

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update B)
Közepes szintű sérülékenység: nem jegyzett keresési út vagy elem.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update A)
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07

ICSA-20-042-02: Siemens Industrial Products SNMP Vulnerabilities (Update B)

Magas szintű sérülékenységek: adatfeldolgozási hiba, nulla pointer dereferencia.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-02

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

ICSA-20-042-10: Siemens SCALANCE S-600 (Update A)
Magas szintű sérülékenységek: ellenőrizetlen erőforrás felhasználás, XSS.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-10

ICSA-19-283-01: Siemens Industrial Real-Time (IRT) Devices (Update D)
Magas szintű sérülékenység: nem megfelelő bementi érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-01

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

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

ICSA-19-099-06: Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update I)
Magas szintű sérülékenység: memória puffer határain kívüli olvasás lehetősége.
https://us-cert.cisa.gov/ics/advisories/ICSA-19-099-06

ICSA-17-339-01: Siemens Industrial Products (Update P)
Magas szintű sérülékenység: nem megfelelő bementi érvényesítés.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01

ICSA-17-243-01: Siemens OPC UA Protocol Stack Discovery Service (Update D)
Magas szintű sérülékenység: XML külső hivatkozás nem megfelelő korlátozása.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-243-01-0

ICSA-17-129-02: Siemens PROFINET DCP (Update R)
Közepes szintű sérülékenység: nem megfelelő bementi érvényesítés.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

ICSA-20-219-01: Trailer Power Line Communications
Közepes szintű sérülékenység: érzékeny információk feltárása a küldött adatokban.
https://us-cert.cisa.gov/ics/advisories/icsa-20-219-01

ICSA-20-219-02: Advantech WebAccess HMI Designer
Kritikus szintű sérülékenységek: puffer túlcsordulás, puffer memória határain kívüli olvasás lehetősége, inicializálási problémák, memória címhívási probléma.

https://us-cert.cisa.gov/ics/advisories/icsa-20-219-02

ICSA-20-219-03: Geutebrück G-Cam and G-Code

Magas szintű sérülékenység: operációs rendszerbe parancs befecskendezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-219-03

ICSA-20-219-04: Delta Industrial Automation TPEditor

Magas szintű sérülékenységek: nem megfelelő bemeneti érvényesítés, puffer túlcsordulás, memória puffer határain kívüli olvasás lehetősége, káros kód feltöltésének lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-20-219-04

ICSA-20-217-01: Delta Industrial Automation CNCSoft ScreenEditor

Magas szintű sérülékenységek: puffer túlcsordulás, puffer memória határain kívüli olvasás lehetősége, nem inicializált mutató használata.
https://us-cert.cisa.gov/ics/advisories/icsa-20-217-01

ICSA-20-168-01: Treck TCP/IP Stack (Update F)

Kritikus szintű sérülékenységek: Hosszparaméterek nem megfelelő kezelése, nem megfelelő bemeneti érvényesítés, memóriacím duplán történő hívása, memória puffer határain kívüli olvasás lehetősége, nem megfelelő hozzáférés ellenőrzés, egészszám túlcsordulás, nem megfelelő érvénytelenítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

ICSMA-20-212-01: Philips DreamMapper

Közepes szintű sérülékenység: érzékeny információk naplófájlba történő beillesztése.
https://us-cert.cisa.gov/ics/advisories/icsma-20-212-01

ICSA-20-212-01: Inductive Automation Ignition 8

Magas szintű sérülékenység: hiányzó engedélyezés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-01

ICSA-20-212-02: Mitsubishi Electric Multiple Factory Automation Engineering Software Products

Magas szintű sérülékenység: engedély problémák.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-02

ICSA-20-212-03: Mitsubishi Electric Factory Automation Products Path Traversal

Magas szintű sérülékenység: útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-03

ICSA-20-212-04: Mitsubishi Electric Factory Automation Engineering Products

Magas szintű sérülékenység: Nem jegyzett keresési út vagy elem.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04

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. augusztus hónapban az ICS-CERT az alábbi riasztást adta ki:

Robot Motion Szerver

A Robot Motion szerver kritikus sérülékenységéről adott ki riasztást az ICS-CERT, amelyet kihasználva egy támadónak lehetősége nyílik káros kód futtatására. A sérülékenység nem használható ki távolról. A riasztás nem kizárólag egy gyártót érint, hanem valamennyi OEM robot érintett, függetlenül attól, hogy nyílt forráskódú vagy sem.

Az ICS-CERT a korai figyelmeztetést azért adta ki, hogy a kockázatok a lehető leghamarabb csökkenthetők legyenek.

A sérülékenység: Az adatok hitelességének nem elégséges ellenőrzése, melynek hatása lehet távoli kód futtatása.

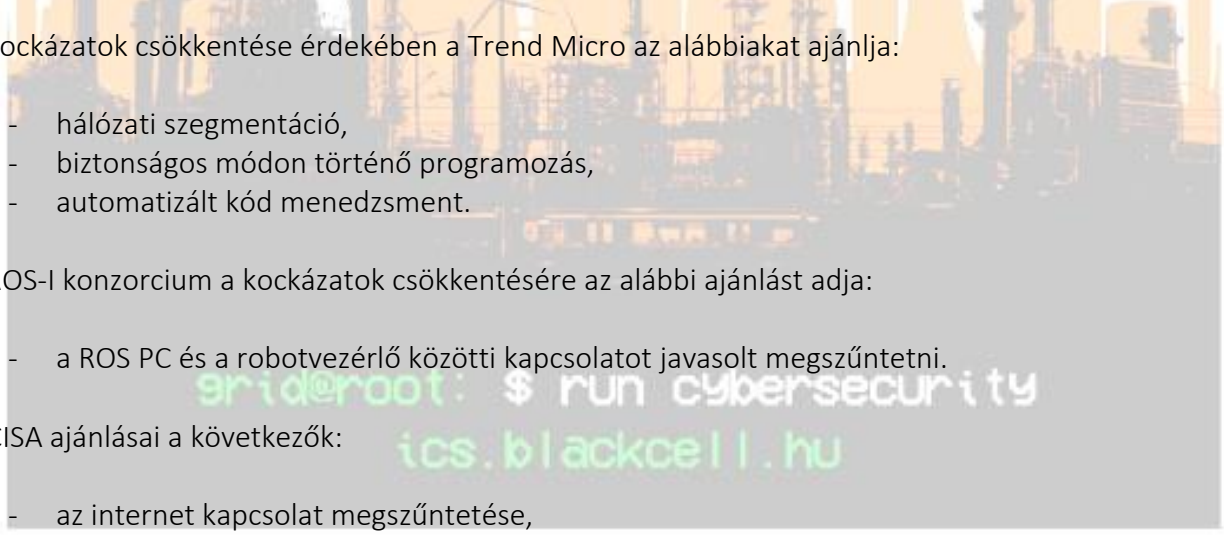
A sérülékenységben érintett ágazatok a következők: gyártó ipar, egészségügy. A sérülékenység abban az esetben használható ki, ha a hozzáférés kontrollok (főként fizikai) nem működnek. A sérülékenység kihasználása hálózati hozzáféréssel és az ipari robotika ismeretivel felruházott támadó számára lehetséges, aki így szenzitív információkat is eltulajdoníthat, vagy zavarhatja a kívánt működést.

A kockázatok csökkentése érdekében a Trend Micro az alábbiakat ajánlja:

- hálózati szegmentáció,
- biztonságos módon történő programozás,
- automatizált kód menedzsment.

A ROS-I konzorcium a kockázatok csökkentésére az alábbi ajánlást adja:

- a ROS PC és a robotvezérlő közötti kapcsolatot javasolt megszűntetni.



A CISA ajánlásai a következők:

- az internet kapcsolat megszűntetése,
- az üzleti hálózatról válassza le a termelési hálózatot,
- ha szükséges távoli hozzáférés, használjon VPN megoldást.

A riasztás részletesebb leírását a következő linken találja meg:

https://us-cert.cisa.gov/ics/alerts/ics-alert-20-217-01

A korábban kiadott riasztások részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

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