9. 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 2

ICS KÉPZÉSEK, OKTATÁSOK 3

ICS KONFERENCIÁK 6

ICS INCIDENSEK 7

KÖNYVAJÁNLÓ 8

BLACK CELL JAVASLATOK 9

ICS SÉRÜLÉKENYSÉGEK 10

ICS RIASZTÁSOK 13

ICS jó gyakorlatok, javaslatok

A SANS Institute által, a Programozható Logikai Vezérlők (PLC) biztonságáról kiadott Whitepaper részletesen taglalja a PLC biztonság bizonyos szegmenseit.

A dokumentum kifejti, hogy nincs egy jó módszer, amely minden egyes PLC biztonságát szolgálhatná, minden esetben más és más szegmenseit kell érinteni a biztonságnak, mely rendkívül sok tényező függvénye. A publikáció azokra a fontos pontokra mutat rá, ahol koncentráltan szükséges a biztonság megteremtése az említett rendszerek vonatkozásában.

A PLC-k csatlakoztatva vannak számos ipari eszközhöz, mely számos kockázatot hordoz magában. A dokumentum klasszifikálja a PLC eszközöket, mely osztályozás a fizikai méret, a csatlakoztatott eszközök száma, és a teljesítmény alapján határozódik meg.

A dokumentum a PLC implementáció 3 típusát is megkülönbözteti, amelyek között szerepel az izolált rendszer, melyben a bemeneti és kimeneti eszközök között foglal helyet a PLC egy izolált rendszerben (Type A). A 2. típus szerint egy belső zárt rendszerben van a PLC, ahol a menedzsment általi bemeneti és kimeneti adatokon túlmenően szerepelnek a termelésben résztvevő eszközök (Type B), és a 3., melyben a menedzsment által megadott adatok külső helyről csatlakozik be a rendszerbe (Type C).

A dokumentum kifejti a PLC-ket érintő fenyegetések és sérülékenységek fajtáit (például: DDoS támadás, vagy spyware-ek, malware-ek stb.).

A különböző fenyegetések és sérülékenységek kockázati szintjét a 3 típusú PLC implementáció vonatkozásában megadja a dokumentum, 3 szintű besorolásban: alacsony, közepes, magas. Példa:

Type of Threat	Category	Type A	Type B	Type C
Spyware/malware authors	Advanced/APT	Low	Medium	High

A dokumentum említi az integritás védelem biztosításának lehetőségeit, melyekhez bizonyos tool-ok is felhasználhatók. A hozzáférés és a hitelesítés is szigorú szabályok szerint szükséges, hogy megvalósuljon, ahogy a kommunikáció védelme is.

A fizikai biztonság tekintetében a PLC vonatkozásban fontos a switchek védelmének biztosítása, ahogy a PLC eszközön lévő kapcsolók elérését biztosító fedél elérésének és hozzáférhetőségének biztosítása.

A különböző méretű- és hálózati típusú PLC-khez táblázatos formában van megadva a fenyegetések, a beépített védelmi szintek és a biztonsági szint kiterjeszthetőségének aspektusai. A védelmi szintek részletezésre kerülnek a dokumentumban.

A különböző PLC-t használó szervezeteknek érdemes a dokumentumot megvizsgálni, és a hiányos védelmi intézkedésekre koncentráltan kialakítani a megfelelő védelmi szinteket.

A dokumentum a következő weboldalról tölthető le:

https://www.sans.org/reading-room/whitepapers/threats/plc-device-security-tailoring-37612

ICS képzések, oktatások

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

2020. februárban a következő tréning, oktatás kerül lebonyolításra az ICS/SCADA biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials SANS; Now Orleans, Louisiana, USA; 2020. február 3-7.
- ICS410: ICS/SCADA Security Essentials SANS; Zurich, Svájc; 2020. február 24-28.

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/ honlapon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során video 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

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 nem kizárólag helyhez kötötten szervez képzéseket az ipari irányító rendszerek biztonságával kapcsolatban, hanem online kurzust is indít:

- ICS410: ICS/SCADA Security Essentials SANS

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

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

ICS konferenciák

A teljesség igénye nélkül a következő konferenciák kerülnek megrendezésre 2020. februárban:

MANUSEC Europe

A 2 napos konferencián a globális és komplex ellátási láncok kapcsolatai és automatizációja, mint a kritikus infrastruktúrák meghatározó kockázata kerül a középpontba. Számos esettanulmányon keresztül mutatják be az előadók, hogy az ICS rendszereket miként védik meg a kibertámadások káros hatásaival szemben, vagy az IT és OT terület együttműködés kultúrájának növekedési tendenciáját.

A rendezvényen kerekasztal beszélgetés keretében szó lesz egy OT biztonsági incidenst követő 48 óra eseményeiről, továbbá szó lesz a bizalom nélküli (Zero Trust) hálózati megközelítésről, az adatok és az eszközök vonatkozásában.

Cyber Security for Critical Maufacturing; München, Németország; 2020. február 4-5.

További részletek a következő webhelyen találhatók:

https://europe.manusecevent.com/?ref=infosec-conferences.com

Driving Digital Transformation in Industry and Cities

A rendezvényen az ipar és infrastruktúra, illetve az okos városok biztonsági kérdései kerülnek terítékre. A fő témák érinteni fogják a felhő, a gépi tanulás, a dolgok internete, a kiberbiztonsági jó gyakorlatok, a DevOps, az IT, OT, ET csapatok képességeit és működését, kapcsolati pontjait.

Az iparban használt blockchain technológia is részletesen bemutatásra kerül, ahogy a kiberbiztonság és az emberi biztonság, vagy az okos eszközök kapcsolatai is.

Driving Digital Transformation in Industry and Cities; Orlando, Florida, USA; 2020. február 3-6.

További részletek a következő webhelyen találhatók:

https://www.arcweb.com/events/arc-industry-forum-orlando

ICS incidensek

Gangnam Industrial Style

Több, mint 200 szervezet esett áldozatul egy APT kampánynak, amely az ipari irányító rendszereket célozta meg.

A CyberX által felfedezett kiber-kémkedésről szóló kampány céljai az ipari, mérnöki, és gyártó üzemi szervezetek, melyek 60%-a Dél-Koreában található. Az áldozatok között található azonban kritikus infrastruktúra üzemeltető is, a kémiai iparból, az energia szállító- és elosztót üzemeltető szervezetekből, továbbá a megújuló energia szektorból is. A további áldozatok a következő országokban találhatók: Törökország, Németország, Egyesült Királyság, Indonézia, Ecuador.

A kampány jellemzően jelszavak és dokumentumok lopásával kezdődik, amelyek kereskedelmi titkokat is tartalmaznak, és előkészítenek egy későbbi támadást, amelyekkel az ipari vezérlők és hálózataik kompromittálhatók, akár ransomware támadással.

Spear-phising technikával és rosszindulatú csatolmánnyal rendelkező e-mailes módszerrel valósul meg a jellemzően Pdf. fájlokat felhasználó támadás, és a csatolmány ipari témájú, mint például erőművekhez kapcsolódó ábrák, Whitepaper-ek stb. Több esetben a nyilvánosan elérhető szervezeti profilok is felhasználásra kerülnek a hatékonyság növelése érdekében. Előfordul, hogy a Siemens leányvállalata által küldött legitim e-mailnek látszik a támadás.

A 2013-ból ismert Sonicwall egy új változatát használják a támadók a cselekményük végrehajtása során. A káros kódot a böngésző és az e-mail hitelesítő adatok gyűjtésére, valamint office dokumentumok és file-ok eltulajdonítására használják.

A fenyegetés folyamatosan fennáll, mert a kutatók rendszeresen új ellopott hitelesítő adatokkal kerülnek szembe a támadók C2 szervere tekintetében.

További információ a következő linken található:

https://securityaffairs.co/wordpress/95289/apt/gangnam-industrial-style-campaign.html

Szerző: Gyakran előfordul, hogy az ipari irányító rendszerek nem közvetlen célpontjai a támadóknak, hanem gyakran megpróbálnak adatokat gyűjteni az ICS rendszerek támadásához, egyszerűbb módszerek segítségével. Ez így sokkal könnyebb feladat, mert az emberi tulajdonságok kihasználása megkönnyíti azon adatok megszerzését, amelyeket felhasználva növelhető a támadás sikeressége.

Előzőekre tekintettel a felhasználói tudatosság meghatározó, és sajnos sok esetben bagatellizálva van a szervezet vezetése részéről, és sok esetben rosszul megszervezettek az információbiztonság tudatossági kampányok, oktatások. Minden a témával foglalkozó előadásban elhangzik, hogy a leggyengébb láncszem az ember, mégsem fordít kellő figyelmet a tudatosság növelésére a szervezetek vezetésének nagytöbbsége.

Könyvajánló

A modern infrastruktúrák fejlődése magával hozza az ipari irányító rendszerek elleni támadásokat is. Új fenyegetések jelennek meg, és a sérülékenységek kihasználásra kerülnek, mellyel a bizalmasság, sértetlenség és rendelkezésre állás követelményei sérülnek.

A helytelen adatok, vagy parancsok befecskendezése is jelen van az ICS rendszerek elleni támadásokban, komplex és kifinomult formában. A támadók hozzáféréseket szerezhetnek a rendszerekhez, kritikus folyamatokhoz, így az ártalmas kódok, parancsok lefuttathatóvá válnak.

A kutatás során integrált automatizációs laborban folyamat-vezérelt rendszert használtak bizonyos paraméterek megszerzése érdekében. A befecskendezéses támadások szimulációja során fals adatok kerültek be az üzemeltetési adatok közé. A 3 rétegű architektúra feladata az adatok minősítése, és annak megállapítása, hogy normál folyamat, vagy támadás zajlik éppen.

A kutatás eredményei azt bizonyítják, hogy az eddig létező mély gépi tanulást is felülmúlja a kísérlet során használt CNN (Convolutional Neural Networks - Konvolúciós neurális hálózatok) használata.

A további részletekért érdemes elolvasni a Studies in Computational Intelligence könyvsorozat részeként 2019. novemberében publikált kiadványt.

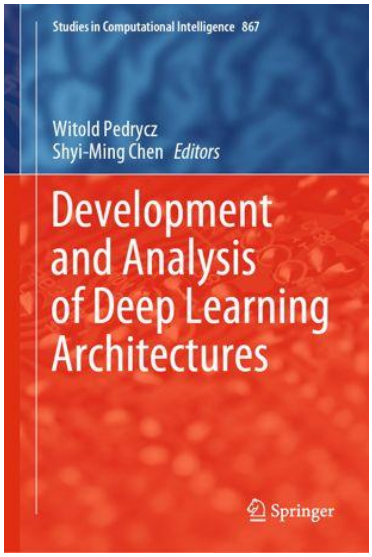
A könyv címe: **Securing Industrial Control Systems from False Data Injection Attacks with Convolutional Neural Networks**

Szerzők: Sasanka Potluri, Shamim Ahmed, Christian Diedrich

Kiadás éve: 2019.

A kiadvány elérhető a következő linken:

https://link.springer.com/chapter/10.1007/978-3-030-31764-5_8



Black Cell javaslatok

A Black Cell 2019. évi 4. hírlevelében bemutatásra került a NIST 800-82 keretrendszer, amely az ipari irányító rendszerek biztonsági útmutatója. A biztonság kialakítása során rengeteg tényezőt figyelembe kell vennie a szervezetnek. Előfordul, hogy a NIST 800-82 hivatkozik más keretrendszerre (ajánlásra), amely segítséget nyújt speciális kérdésekben, vagy a módszertanban megfogalmazottak más ajánlással együtt lesznek teljeskörűek.

A következő ajánlásokat említi a módszertan, amelyek bizonyos szakterületek sajátosságait részletesebben kifejtik (szintén NIST ajánlások, melyek ingyenesen hozzáférhetők):

- NIST 800-63 (távoli elektronikus hitelesítés)
- NIST 800-48 (hálózat nélküli kapcsolatok biztonsága (bluetooth standardok))
- NIST 800-97 (IEEE 802.11i hálózat nélküli biztonság)
- FIPS 201 (személyes identitás azonosítás)
- NIST 800-96 (személyes azonosító kártya olvasó interoperabilitás)
- NIST 800-73 (személyes identitás azonosítás interfészen keresztül)
- NIST 800-76 (biometrikus hitelesítés)
- NIST 800-78 (kriptográfiai algoritmusok és kulcs a személyes azonosításhoz – token alapú hitelesítés)
- NIST SP 800-50 (a biztonság tudatossági oktatásokról)
- NIST SP 800-100 (információbiztonsági szabályozás és tervezés)
- NIST 800-61 (segítséget nyújt az incidens kezelési és audit log megőrzési feladatokról)
- NIST 800-92 (a log menedzsmentről)
- NIST SP 800-70 (IT termékek konfigurációs beállításai)
- NIST SP 800-128 (biztonság központú konfiguráció menedzsment program implementálása)
- NIST 800-37 (az információs rendszer határainak megállapításához, biztonsági akkreditációjához)
- NIST SP 800-34 (vészhelyzeti tervezés)
- NIST 800-83 (malware okozta incidens megelőzése és kezelése)
- NIST 800-88 (az eszközök törlésével kapcsolatos technikák és eljárások)
- NIST 800-46 (távmunka és a szélessávú kommunikáció biztonsága)

Az említett ajánlások nem kizárólag az ICS rendszerek biztonságát hivatottak biztosítani, de kétségkívül segítséget nyújtanak ICS környezetben is, hogy azok a biztonság szempontjából fontos sarokpontok azonosításra kerüljenek, és a védelem megfelelő szintre történő fejlesztése megvalósulhasson.

Javasoljuk az ajánlások használatát a biztonság kialakítása vagy fejlesztése során!

ICS sérülékenységek

2020. januárjában 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:

ICSMA-20-023-01: **GE CARESCAPE, ApexPro, and Clinical Information Center systems**

Kritikus szintű sérülékenységek: hitelesítő adatok nem védett formában történő tárolása, nem megfelelő bemeneti hitelesítés, beégetett hitelesítő adatok használata, kritikus funkciók nem megfelelő hitelesítése, nem megfelelő erősségű titkosítás, veszélyes fájltípus feltöltés korlátozás hiánya.
https://www.us-cert.gov/ics/advisories/icsma-20-023-01

ICSA-20-021-01: **Honeywell Maxpro VMS & NVR**

Kritikus szintű sérülékenységek: nem megbízható adatok ellenőrzésének hiánya, SQL befecskendezés.
https://www.us-cert.gov/ics/advisories/icsa-20-021-01

ICSA-20-016-01: **Schneider Electric Modicon Controllers**

Magas szintű sérülékenység: nem megfelelő feltétel ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-016-01

ICSA-20-014-01: **GE PACSystems RX3i**

Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-014-01

ICSA-20-014-02: **Siemens SINEMA Server**

Kritikus szintű sérülékenység: hibás privilégium kezelés.
https://www.us-cert.gov/ics/advisories/icsa-20-014-02

ICSA-20-014-03: **Siemens SCALANCE X Switches**

Magas szintű sérülékenység: kritikus funkció hiányzó hitelesítése.
https://www.us-cert.gov/ics/advisories/icsa-20-014-03

ICSA-20-014-04: **Siemens SINAMICS PERFECT HARMONY GH180**

Közepes szintű sérülékenység: védelmi mechanizmus hibája.
https://www.us-cert.gov/ics/advisories/icsa-20-014-04

ICSA-20-014-05: **Siemens TIA Portal**

Magas szintű sérülékenység: útvonal bejárás.
https://www.us-cert.gov/ics/advisories/icsa-20-014-05

ICSA-20-014-06: **OSIsoft PI Vision**

Magas szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, CSRF, XSS, érzékeny adatok log fájlokba történő felvétele.
https://www.us-cert.gov/ics/advisories/icsa-20-014-06

ICSA-19-344-07: Siemens EN100 Ethernet Module (Update A)
Magas szintű sérülékenységek: memória pufferen belüli műveletek nem megfelelő korlátozása, XSS, útvonal bejárás.
https://www.us-cert.gov/ics/advisories/icsa-19-344-07

ICSA-19-283-01: Siemens Industrial Real-Time (IRT) Devices (Update A)
Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-283-01

ICSA-19-283-02: Siemens PROFINET Devices (Update B)
Magas szintű sérülékenység: nem megfelelő erőforrás kezelés.
https://www.us-cert.gov/ics/advisories/icsa-19-283-02

ICSA-19-281-03: Siemens SIMATIC WinAC RTX (F) 2010 (Update A)
Magas szintű sérülékenység: nem megfelelő erőforrás kezelés.
https://www.us-cert.gov/ics/advisories/icsa-19-281-03

ICSA-19-162-04: Siemens SCALANCE X (Update A)
Magas szintű sérülékenység: jelszavak visszaállítható formában történő tárolása.
https://www.us-cert.gov/ics/advisories/ICSA-19-162-04

ICSA-19-099-03: Siemens Industrial Products with OPC UA (Update D)
Magas szintű sérülékenység: nem megfelelő kivétel kezelés.
https://www.us-cert.gov/ics/advisories/ICSA-19-099-03

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

ICSA-19-085-01: Siemens SCALANCE X (Update B)
Közepes szintű sérülékenység: API vagy funkció nem az elvártnak megfelelő viselkedése.
https://www.us-cert.gov/ics/advisories/ICSA-19-085-01

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

ICSA-18-163-02: Siemens SCALANCE X Switches (Update A)
Közepes szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/ICSA-18-163-02

ICSMA-19-274-01: Interpeak IPnet TCP/IP Stack (Update D)
Kritikus szintű sérülékenységek: puffer túlcsordulás, egész szám túlcsordulás, memória pufferen belüli műveletek nem megfelelő korlátozása, null pointer dereferencia, parancs kezelési hiba.
https://www.us-cert.gov/ics/advisories/icsma-19-274-01

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

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

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