2023 February, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you’re interested in ICS security, feel free to contact our experts at info@blackcell.io.

List of Contents

ICS good practices, recommendations

The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures

Critical Infrastructures business continuity is a key success indicator. The past few years the environment and the threat landscape changed. Analysing the following survey is strongly recommended!

Abstract

Among the many repercussions of the COVID-19 emergency to be assessed, those on critical infrastructures and the associated businesses and professions are certainly important ones. In this paper, we document the conception, implementation and outcome of a survey organized by European Commission’s Joint Research Centre and entitled “COVID-19: Emergency & Business Continuity”. This was conducted in April-May 2020 with the participation of critical infrastructure experts (including professionals from the academia and research institutions, infrastructure operators and industry representatives, public authorities and members of security agencies), involved as stakeholders in the European Reference Network for Critical Infrastructure Protection (ERNCIP). Themes explored through this study include an assessment of the business continuity status and the evaluation of emergency management and disaster recovery aspects, as experienced from the perspective of different sectors, organization types and personal perceptions of the respondents.

Source (the survey) and more information available on the following link:

https://www.sciencedirect.com/science/article/pii/S0925753521000047?via%253Dihub

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in March 2023:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

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

- Industrial Control System (ICS) & SCADA Cyber Security Training

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- ICS/SCADA security training seminar

https://www.enoinstitute.com/scada-ics-security-training-seminar/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

ICS conferences

In March 2023, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

Critical Infrastructure Protection & Resilience North America

The ever-changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber-attacks, means the need to continually review and update policies, practices and technologies to meet these growing demands.

Preliminary Conference Programme Critical Infrastructure Protection and Resilience North America will bring together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

Baton Rouge, Louisiana, USA; 7th – 9th March 2023

More details can be found on the following website:

https://ciprna-expo.com/

Smart Grid Technical Innovations in: Digital Substations | SCADA & Control Centres | Utility Telecoms | Cybersecurity

This week-long conference draws together 200+ smart grid technical professionals for a review of grid innovation projects in the context of increased regulatory pressures, intense cybersecurity threats, and rapidly rising demand for renewables integration.

The week begins with a practical workshop focused on one of the most crucial IEC standards for the smart grid: IEC 61850 for Substation Automation. Led by Christoph Brunner, Convenor of TC57 WG10, this is a great opportunity to get up to speed with the latest evolutions and applications of the standard. The main 3-day conference opens with a morning of plenary sessions addressing the big macro issues affecting the Energy Transition, and then breaks out into three technical tracks focused on innovations in Digital Substations, SCADA and Control Centres, and Utility Telecoms. The week wraps up with a future-focused briefing on smart grid cybersecurity, addressing everything from the threat landscape to innovations in prevention, detection and response strategies.

Amsterdam, Netherlands; 20th – 24th March 2023

More details can be found on the following website:

https://industrialcyber.co/event/smart-grid-technical-innovations-in-digital-substations-scada-control-centres-utility-telecoms-cybersecurity/

2023 Industrial Control Systems (ICS) Security Symposium series

Public Safety Canada also periodically hosts a focused information session, including presentations and facilitated discussions, for those unfamiliar with the complexities of ICS security. The objective of this foundational session is to provide new skills to Canadian critical infrastructure (CI) personnel including management, senior officials, and anyone working at CI sites where ICS are employed. We encourage those responsible for infrastructure security to attend in order to broaden their knowledge of the impacts and issues facing ICS today.

Topics covered in this session include:

- What is ICS?: An Introductory Overview
- Information Technology vs. Operational Technology (IT/OT)
- Where ICS is Found: A Walkthrough of ICS in the Water Sector From Water Source to Faucet
- Case Studies of ICS Cyber Events
- Public Safety Canada Resources Available to the CI Community

Miami South Beach, USA; 29th March 2023

More details can be found on the following website:

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/index-en.aspx

ICS incidents

Russian Hackers Disrupt NATO Earthquake Relief Operations

Killnet claims DDoS attack against NATO Special Operations Headquarters, Strategic Airlift Capability, and more.

NATO's Special Operations Headquarters and Strategic Airlift Capability — both working to deliver humanitarian aid to victims of the recent Turkish-Syrian earthquake — were among NATO organizations disrupted by a weekend cyberattack.

Russian-based Killnet threat group has claimed responsibility for launching distributed denial-of-service (DDoS) attacks against NATO, according to reports.

"We are carrying out strikes on NATO," Killnet wrote on its Telegram channel, according to The Telegraph.

Reports added NATO's NR network, reportedly used to transmit sensitive and classified data, was also targeted. Besides knocking sites temporarily offline, the cyberattack disrupted communications between NATO and at least one of its airplanes transporting search and rescue equipment to Incirlik Air Base in Turkey, The Telegraph reported.

A devastating earthquake hit in southeastern Turkey and Syria on Feb, 6 and along with its aftershocks. has already claimed 35,000 lives. Emergency workers from around the world have converged on the area to join in efforts to pull survivors from the rubble.

"NATO cyber experts are actively addressing an incident affecting some NATO websites," a NATO spokesperson told The Telegraph confirming the hack. "NATO deals with cyber incidents on a regular basis, and takes cyber security very seriously."

The source is available on the following link:

https://www.darkreading.com/attacks-breaches/russian-hackers-disrupt-nato-earthquake-relief-operations-

Book recommendation

A Comprehensive Guide to Operational Technology (OT) Cybersecurity

Operational technology (OT) cybersecurity references the software, hardware, practices, personnel, and services deployed to protect operational technology infrastructure, people, and data.

As data collection and analysis become more important, technology continually changes, and "big data" is enabled through the IT/OT convergence, it has become necessary to reassess cybersecurity best practices for protecting OT.

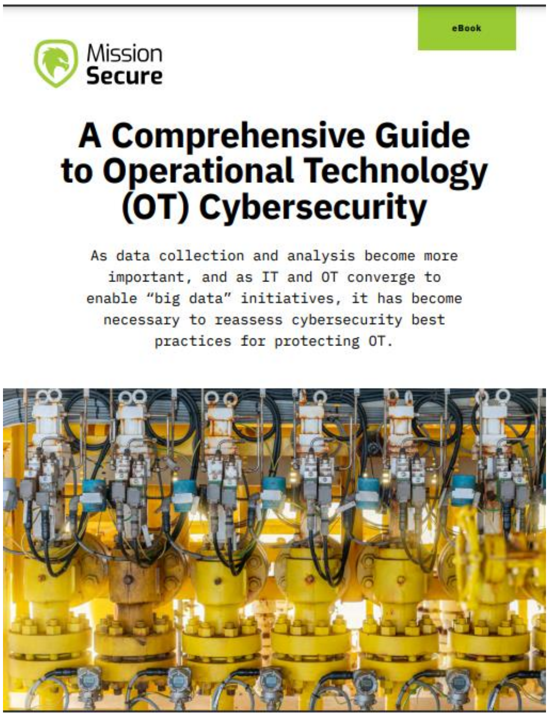
In this guide, we'll explore how OT cybersecurity was established, where it's at, current best practices, and the top trends hinting at what's next — allowing you to better prepare and implement your cybersecurity action plan.

Authors/Editors: Mission Secure

Year of issue: 2022

The book is available at the following link:

https://www.missionsecure.com/resources/comprehensive-guide-to-operational-technology-security-ebook



eBook

Mission Secure

A Comprehensive Guide to Operational Technology (OT) Cybersecurity

As data collection and analysis become more important, and as IT and OT converge to enable "big data" initiatives, it has become necessary to reassess cybersecurity best practices for protecting OT.

ICS security news selection

Cyber Insights 2023 | ICS and Operational Technology

Recognition of the cyber threat to industrial control systems (ICS) and operational technology (OT) systems has grown over the last decade. Until recently, this has been largely a theoretical threat founded on the danger of what could happen rather than what is happening. This is changing, and the threat to ICS/OT is now real and ongoing. The bigger danger is that this is likely to increase in 2023 and onward.

There are several reasons, including geopolitical fallout and escalation of tensions from the Russia/Ukraine war, and a growing willingness of criminals to target the ICS of critical industries. At the same time, ICS/OT is facing an expanding attack surface caused by continuing business digitization, an explosion of IoT and IIoT devices, the coming together of IT and OT networks, and the use of potentially insecure open source software libraries to bind it all together. …

Source, and more information:

https://www.securityweek.com/cyber-insights-2023-ics-and-operational-technology/

Pro-Palestine hackers threaten Israeli chemical companies

Threat actors are targeting Israeli chemical companies operating in the occupied territories, security experts warn.

Threat actors have launched a massive hacking campaign aimed at Israeli chemical companies operating in the occupied territories. A group, named Electronic Quds Force, is threatening companies' engineers and workers and are inviting them to resign from their positions.

The attacks are retaliation against the Israeli government and its policy against Palestinians, the hackers accuse Tel Aviv of violence.

"*Our advice to scientists working in the chemical plants is to quit their job, hunt for a new one, and find sanctuary in a location where we are not present,*" the message sent by the Electronic Quds Force. "*Leave their employment. Look for a new one.*" "*This is while we have a strong presence anyplace,*" …

Source, and more information:

https://securityaffairs.com/141609/cyber-warfare-2/cyber-attacks-israeli-chemical-companies.html

The Journey of Endpoint Security in ICS Cybersecurity – From Old-School to Next-Gen

The evolution of endpoint security in industrial control systems (ICS) cybersecurity has been a continuous process to keep up with the changing threat landscape. With the increasing use of connected devices and the rise of advanced threats, the need for robust endpoint security has become critical. In this blog, we will discuss the evolution of security on the endpoint in ICS, the types of solutions, their advantages and disadvantages, and the factors that need to be considered while deploying.

Older Solutions

Endpoint security started as antivirus software, which was used to detect and remove malware from individual computers. Earlier there were few options available, simply antivirus was there, and sometimes anti-spyware and anti-adware were also possible. However, as the threat landscape evolved, the need for more sophisticated security solutions became evident. …

Source, and more information:

https://industrialcyber.co/end-point-hmi-security/the-journey-of-endpoint-security-in-ics-cybersecurity-from-old-school-to-next-gen/

Critical Infrastructure at Risk from New Vulnerabilities Found in Wireless IIoT Devices

A set of 38 security vulnerabilities has been uncovered in wireless industrial internet of things (IIoT) devices from four different vendors that could pose a significant attack surface for threat actors looking to exploit operational technology (OT) environments.

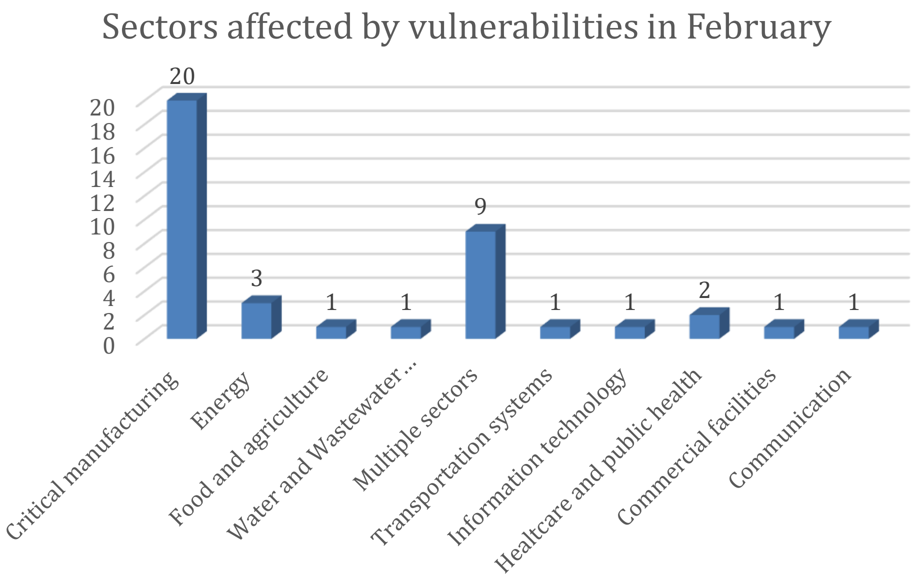
"Threat actors can exploit vulnerabilities in Wireless IIoT devices to gain initial access to internal OT networks," Israeli industrial cybersecurity company Otorio said. "They can use these vulnerabilities to bypass security layers and infiltrate target networks, putting critical infrastructure at risk or interrupting manufacturing." …

Source, and more information:

https://thehackernews.com/2023/02/critical-infrastructure-at-risk-from.html

ICS vulnerabilities

In February 2023, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

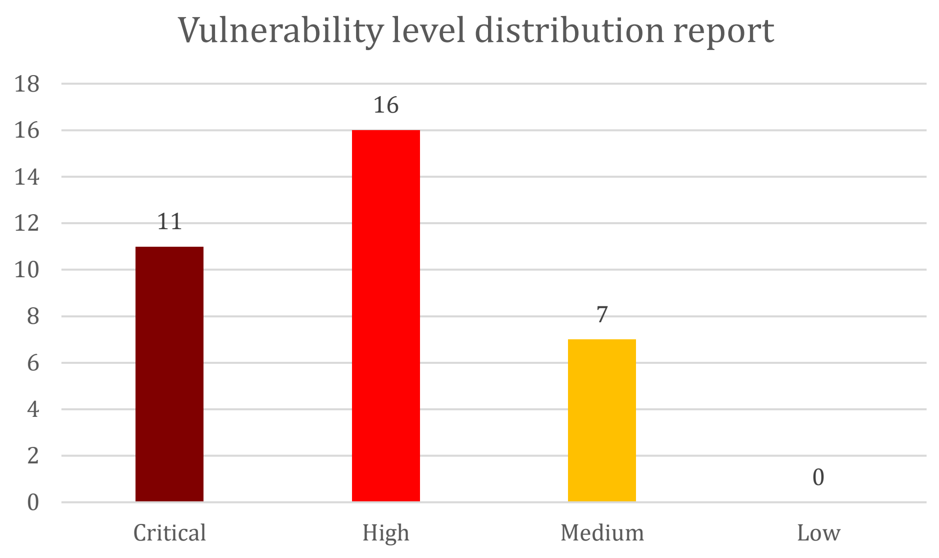


Average number of vulnerabilities per vulnerability report in February: **2,56**

Vulnerabilities/Exploitable remotely: **34/22**

The most common vulnerabilities in February:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	6
Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE-119	5
Out-of-bounds Write	CWE-787	5
OS Command Injection	CWE-78	4
Out-of-bounds Read	CWE-125	4
Cross-site Scripting	CWE-79	4
Stack-based Buffer Overflow	CWE-121	4



ICSA-23-059-01: **Hitachi Energy Gateway Station**

High level vulnerabilities: NULL Pointer Dereference, Infinite Loop.

Hitachi Energy Gateway Station | CISA

ICSA-23-059-02: **Hitachi Energy Gateway Station**

High level vulnerabilities: Improper Input Validation, Classic Buffer Overflow.

Hitachi Energy Gateway Station | CISA

ICSA-22-139-01: **Mitsubishi Electric MELSEC iQ-F Series (Update B)**

High level vulnerability: Improper Input Validation.

Mitsubishi Electric MELSEC iQ-F Series (Update B) | CISA

ICSA-23-054-01: **PTC ThingWorx Edge**

Critical level vulnerabilities: Improper Validation of Array Index, Integer Overflow or Wraparound.

PTC ThingWorx Edge | CISA

ICSA-23-052-01: **Mitsubishi Electric MELSOFT iQ AppPortal**

Critical level vulnerabilities: HTTP Request Smuggling, Insufficient Verification of Data Authenticity.

Mitsubishi Electric MELSOFT iQ AppPortal | CISA

ICSMA-21-187-01: **Philips Vue PACS (Update C)**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Improper Authentication, Improper Initialization, Use of a Broken or Risky Cryptographic Algorithm, Protection Mechanism Failure, Use of a Key Past its Expiration Date, Insecure Default Initialization of Resource, Improper Handling of Unicode Encoding, Insufficiently Protected Credentials, Data Integrity Issues, Cross-site Scripting, Improper Neutralization, Use of Obsolete Function, Relative Path Traversal.

Philips Vue PACS (Update C) | CISA

ICSA-23-047-01: **Siemens Solid Edge**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Heap-based Buffer Overflow, Stack-based Buffer Overflow, Access of Uninitialized Pointer, Improper Restriction of Operations within the Bounds of a Memory Buffer, Use After Free.

Siemens Solid Edge | CISA

ICSA-23-047-02: **Siemens SCALANCE X200 IRT**

High level vulnerability: Improper Input Validation.

Siemens SCALANCE X200 IRT | CISA

ICSA-23-047-03: **Siemens Brownfield Connectivity Client**

Critical level vulnerabilities: OS Command Injection, Improper Certificate Validation, Use of a Broken or Risky Cryptographic Algorithm, Improper Resource Shutdown or Release.

Siemens Brownfield Connectivity Client | CISA

ICSA-23-047-04: **Siemens Brownfield Connectivity Gateway**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Uncontrolled Resource Consumption, Exposure of Resource to Wrong Sphere, Allocation of Resources without Limits or Throttling, Improper Certificate Validation.

Siemens Brownfield Connectivity Gateway | CISA

ICSA-23-047-05: **Siemens SiPass integrated AC5102 / ACC-G2 and ACC-AP**

High level vulnerability: Improper Input Validation.

Siemens SiPass integrated AC5102 / ACC-G2 and ACC-AP | CISA

ICSA-23-047-06: **Siemens Simcenter Femap before V2023.1**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.

Siemens Simcenter Femap before V2023.1 | CISA

ICSA-23-047-07: **Siemens TIA Project-Server formerly known as TIA Multiuser Server**

Medium level vulnerability: Untrusted Search Path.

Siemens TIA Project-Server formerly known as TIA Multiuser Server | CISA

ICSA-23-047-08: **Siemens RUGGEDCOM APE1808**

High level vulnerability: Time-of-check Time-of-use (TOCTOU) Race Condition.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-23-047-09: **Siemens SIMATIC Industrial Products**

High level vulnerability: Time-of-check Time-of-use (TOCTOU) Race Condition.

Siemens SIMATIC Industrial Products | CISA

ICSA-23-047-10: **Siemens COMOS**

Critical level vulnerability: Classic Buffer Overflow.

Siemens COMOS | CISA

ICSA-23-047-11: **Siemens Mendix**

Medium level vulnerability: Improper Access Control.

Siemens Mendix | CISA

ICSA-23-047-12: **Siemens JT Open, JT Utilities, and Parasolid**

High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Read.

Siemens JT Open, JT Utilities, and Parasolid | CISA

ICSA-23-047-13: **Sub-IoT DASH 7 Alliance Protocol stack implementation**

Medium level vulnerability: Out-of-bounds Write.

Sub-IoT DASH 7 Alliance Protocol stack implementation | CISA

ICSA-22-298-06: **Delta Electronics DIAEnergie (Update B)**

High level vulnerabilities: Cross-site Scripting, SQL Injection, Authorization Bypass.

Delta Electronics DIAEnergie (Update B) | CISA

ICSMA-23-047-01: **BD Alaris Infusion Central**

High level vulnerability: Credentials Management Errors.

BD Alaris Infusion Central | CISA

ICSA-23-045-01: **Weintek EasyBuilder Pro cMT Series**

Critical level vulnerability: Path Traversal: '\..\filename'.

Weintek EasyBuilder Pro cMT Series | CISA

ICSA-23-040-01: **Control By Web X-400, X-600M**

Critical level vulnerabilities: Cross-Site Scripting, Code Injection.

Control By Web X-400, X-600M | CISA

ICSA-23-040-02: **LS ELECTRIC XBC-DN32U**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Access Control, Cleartext Transmission of Sensitive Information, Access of Memory Location After End of Buffer.

LS ELECTRIC XBC-DN32U | CISA

ICSA-23-040-03: **Johnson Controls System Configuration Tool (SCT)**

High level vulnerabilities: Sensitive Cookie Without ‘HttpOnly’ Flag, Sensitive Cookie in HTTPS Session Without 'Secure' Attribute.

Johnson Controls System Configuration Tool (SCT) | CISA

ICSA-23-040-04: **Horner Automation Cscape Envision RV**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.

Horner Automation Cscape Envision RV | CISA

ICSA-22-179-02: **Omron SYSMAC CS/CJ/CP Series and NJ/NX Series (Update A)**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Insufficient Verification of Data Authenticity, Plaintext Storage of a Password.

Omron SYSMAC CS/CJ/CP Series and NJ/NX Series (Update A) | CISA

ICSA-22-354-03: **ARC Informatique PcVue (Update A)**

Medium level vulnerabilities: Cleartext Storage of Sensitive Information, Insertion of Sensitive Information into Log File.

ARC Informatique PcVue (Update A) | CISA

ICSA-23-037-01: **EnOcean SmartServer**

Medium level vulnerability: Use of Hard-coded Credentials.

EnOcean SmartServer | CISA

ICSA-23-033-01: **Delta Electronics DIAScreen**

High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write.

Delta Electronics DIAScreen | CISA

ICSA-23-033-02: **Mitsubishi Electric GOT2000 Series and GT SoftGOT2000**

Medium level vulnerabilities: Authentication Bypass by Spoofing, Improper Restriction of Rendered UI Layers or Frames.

Mitsubishi Electric GOT2000 Series and GT SoftGOT2000 | CISA

ICSA-23-033-03: **Baicells Nova**

Critical level vulnerability: Command Injection.

Baicells Nova | CISA

ICSA-23-033-04: **Delta Electronics DVW-W02W2-E2**

Critical level vulnerability: OS Command Injection.

Delta Electronics DVW-W02W2-E2 | CISA

ICSA-23-033-05: **Delta Electronics DX-2100-L1-CN**

Critical level vulnerabilities: OS Command Injection, Cross-site Scripting.

Delta Electronics DX-2100-L1-CN | CISA

ICSA-22-221-01: **Mitsubishi Electric Multiple Factory Automation Products (Update D)**

Critical level vulnerabilities: Infinite Loop, OS Command Injection.

Mitsubishi Electric Multiple Factory Automation Products (Update D) | CISA

ICSA-23-031-01: **Delta Electronics DOPSoft**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write.

Delta Electronics DOPSoft | CISA

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

In February 2023, ICS-CERT has published an alert:

Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Health and Human Services (HHS), the Republic of Korea (ROK) National Intelligence Service (NIS), and the ROK Defense Security Agency (DSA) (hereafter referred to as the “authoring agencies”) are issuing this joint Cybersecurity Advisory (CSA) to highlight ongoing ransomware activity against Healthcare and Public Health Sector organizations and other critical infrastructure sector entities.

This CSA provides an overview of Democratic People’s Republic of Korea (DPRK) state-sponsored ransomware and updates the July 6, 2022, joint CSA North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector. This advisory highlights TTPs and IOCs DPRK cyber actors used to gain access to and conduct ransomware attacks against Healthcare and Public Health (HPH) Sector organizations and other critical infrastructure sector entities, as well as DPRK cyber actors’ use of cryptocurrency to demand ransoms.

The authoring agencies assess that an unspecified amount of revenue from these cryptocurrency operations supports DPRK national-level priorities and objectives, including cyber operations targeting the United States and South Korea governments—specific targets include Department of Defense Information Networks and Defense Industrial Base member networks. The IOCs in this product should be useful to sectors previously targeted by DPRK cyber operations (e.g., U.S. government, Department of Defense, and Defense Industrial Base). The authoring agencies highly discourage paying ransoms as doing so does not guarantee files and records will be recovered and may pose sanctions risks.

Published IoC’s:

File Name	**MD5 Hash**
xpopup.rar	1f239db751ce9a374eb9f908c74a31c9
X-PopUp.exe	6fb13b1b4b42bac05a2ba629f04e3d03
X-PopUp.exe	cf8ba073db7f4023af2b13dd75565f3d
xpopup.exe	4e71d52fc39f89204a734b19db1330d3
x-PopUp.exe	43d4994635f72852f719abb604c4a8a1
xpopup.exe	5ae71e8440bf33b46554ce7a7f3de666

Source and more information:

#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities | CISA

North Korea Cyber Threat Overview and Advisories | CISA