# 2021. July, 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, furthermore 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 cara@blackcell.hu.

## List of Contents

# ICS good practices, recommendations

## ENISA publication: PSIRT Expertise and Capabilities Development

The European Union Agency for Cybersecurity published a Health and Energy PSIRT study and recommendations document in June 2020.

PSIRT is a Product Security Incident Response Team is an entity which, at its core, responds to cybersecurity vulnerability reports within the products and services provided by an organisation.

The PSIRT activity uses a methodology, and the publication introduces it.


This five-step approach is helping to navigate between the tasks.

The publication describes the Software Development Life Cycle relevance, and the key findings (PSIRT activities, Third-party vulnerability management platforms, KPIs, Skills, Impact of NIS Directive, Collaboration between PSIRTs, Collaboration between PSIRTs and CSIRTs, PSIRT/CSIRT complementarity within a company, Sectoral distribution, PSIRT activities presentation, PSIRT visibility, External guidance, and support.

The document gives some recommendations in the following topics:

- Security and Agility
- Multidisciplinary team
- Standard vulnerability information exchanges
- Communication between PSIRTs and OES
- PSIRT community events
- ENISA guidance
- PSIRT presentation standardisation
- PSIRT directory
- Reputation & recognition



The document published the used questionnaire and the results of the survey. Many critical infrastructure sectors can use the document to develop the Incident Response teams capabilities.

The source and more information are available on the following link:

https://www.enisa.europa.eu/publications/csirt-expertise-and-capabilities-development

## ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in August 2021:

SANS provides online ICS security courses. The details of the trainings and courses are available on the following link:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

### Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization
- Industrial IoT on Google Cloud Platform
- Emerging Technologies: From Smartphones to IoT to Big Data Specialization
- CAD and Digital Manufacturing Specialization

More details can be found on the following website:

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

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

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

**ICS-CERT Virtual Learning Portal** (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours

- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour NEW

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
  - 9-14. August 2021
  - 14-19. August 2021
  - 23-28. August 2021
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 1-5. August 2021
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security



More details can be found on the following website:

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

The Department of Homeland Security's two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

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

SCADAhacker-com website provides ICS security online courses:

- Understanding, Assessing and Securing Industrial Control Systems

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP, CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

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

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

This is a 3 Days Course, which is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

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

grid@root: $ run cybersecurity
ics.blackcell.hu

# ICS conferences

In August 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

## International Conference on Industrial Control Systems Security ICICSS

15. International Conference on Industrial Control Systems Security aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Industrial Control Systems Security. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Industrial Control Systems Security.

Thailand, Bangkok; 19-20. August 2021

More details can be found on the following website:

https://conferenceindex.org/event/international-conference-on-industrial-control-systems-security-icicss-2021-august-bangkok-th

## Panel Discussion: Industrial Cybersecurity in the Power/Water Industries

Join the final session of the power/water industry webinar spotlight trifecta. Cybersecurity crosses all borders and boundaries. Hear from a panel of industry experts discussing current real-world scenarios and strategies for defending these environments as the operators continue to safeguard the highly critical infrastructure.

Part of the 2021 Process Industry Virtual Conference; 17. August 2021

More details can be found on the following website:

https://register.gotowebinar.com/register/947767344046599952

# ICS incidents

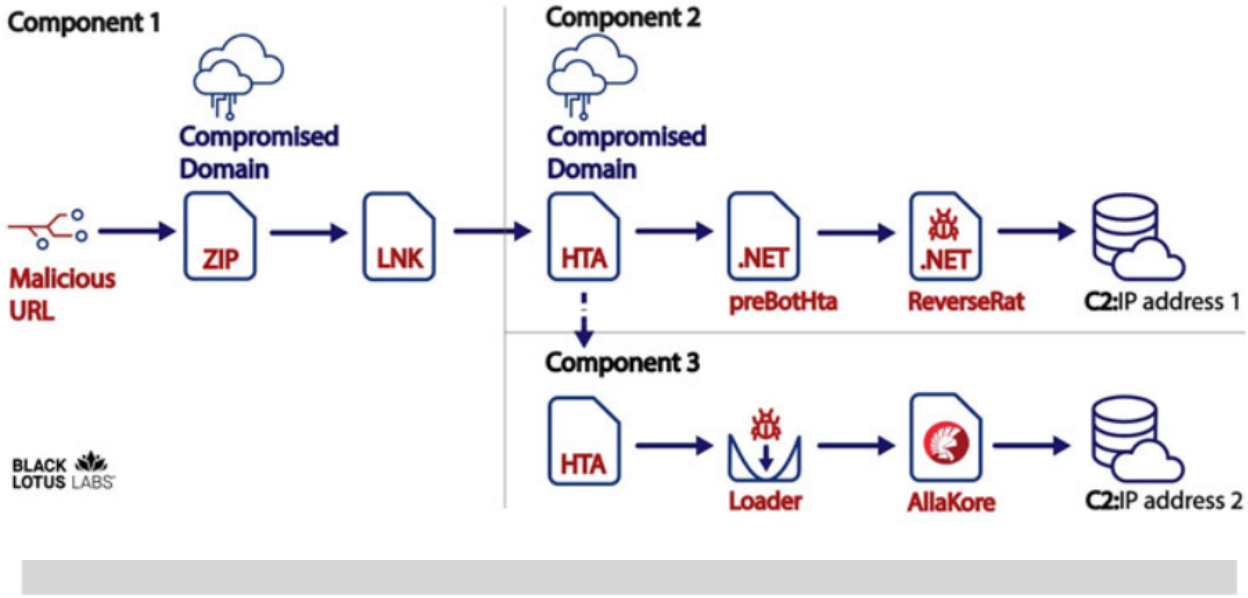
## Eastern power companies targeted by the ReverseRat malware

The Hacker News published an article, which detailed, how the Pakistan-linked hackers attacked Indian and southern Asian power companies.

The targeted systems were Windows-based ones where the threat actor deployed a remote access trojan. The targeted companies were in the following industries: power transmission and power generation and transmission.

The motivation of the hackers is not clear, but the group has been careful to hide their activity by modifying the registry keys, granting them the ability to covertly maintain persistence on the target device without attracting attention.

Explaining the multi-step infection chain, Lumen noted the campaign "resulted in the victim downloading two agents; one resided in-memory, while the second was side-loaded, granting threat actor persistence on the infected workstations.




The malicious links came from phishing e-mails, which when clicked, downloaded a ZIP archive file containing a Microsoft shortcut file (.lnk) and a decoy PDF file from a compromised domain.

This brief incident report tries to draw attention to the ReverseRat project and introduces some details. In July 2021, Tomas Meskauskas published, how to remove ReverseRat from the infected systems.

Sources and more details can be found on the following website:

https://thehackernews.com/2021/06/pakistan-linked-hackers-targeted-indian.html

# Book recommendation

## Industry 4.0 for Process Safety: Handbook

The Chemical industry has been using the same decision guidance tools to manage process safety for the last several decades. During this time there has been exponential growth in the amount of data collected at each site. In 1990 the cost of a gigabyte of storage was $100,000; today it is less than 10 cents.

The tools available for Industry 4.0 enable us to leverage inexpensive sensors, data, and analytics to make far better decisions on how we allocate resources. This means far better process safety for significantly less money. This requires us to challenge the way we have managed process safety in the past and develop a culture shift to support the Digital High Reliability Organization.

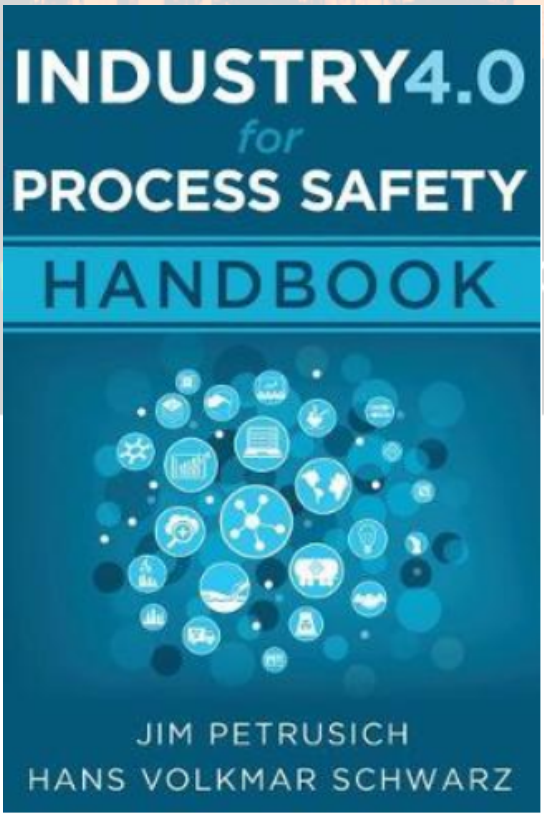
Authors/Editors: Jim Petrusich; Hans Volkmar Schwarz

Year of issue: 2017

The book is available at the following links:

https://www.abe.pl/en/book/9781979021166/industry-40-for-process-safety-handbook

https://www.amazon.ae/Industry-4-0-Process-Safety-Handbook/dp/1979021163



# Black Cell recommendations

## New Ransomware Self-Assessment Security Audit Tool released by CISA

The US Cybersecurity and Infrastructure Security Agency (CISA) has released the Ransomware Readiness Assessment (RRA), a new module for its Cybersecurity Assessment Tool (CSET).

RRA is a security audit self-assessment tool for organizations that want to better understand how well they are equipped to defend and recover from ransomware attacks targeting their information technology (IT), operational technology (OT), or industrial control system (ICS) assets.

This CSET The RRA module was adapted to assess different levels of preparedness for ransomware threats to be useful for all organizations, regardless of their cybersecurity maturity.

“The RRA also provides a clear path for improvement and contains an evolving progression of questions categorized as basic, intermediate, and advanced,” CISA He says on the tool’s wiki page.

“This is intended to help an organization improve by focusing on the basics first and then progressing by implementing practices across the intermediate and advanced categories.”

CISA says the RRA can be used to defend against this growing threat by effectively:

- It helps organizations assess their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
- Guides asset owners and operators through a systematic process to assess their operational technology (OT) and information technology (IT) network security practices against the threat of ransomware.
- It provides an analysis panel with graphs and tables that present the results of the evaluation in summary and detailed form.



Source and more information are available at the following link:

https://news-block.com/cisa-releases-new-ransomware-self-assessment-security-audit-tool/

## ICS vulnerabilities

In July 2021, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSA-21-194-01: **Schneider Electric C-Bus Toolkit**
Medium level vulnerability: Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-01

ICSA-21-194-02: **Schneider Electric SCADApack RTU, Modicon Controllers, and Software**
High level vulnerabilities: Insufficiently Protected Credentials, Authentication Bypass by Spoofing, Deserialization of Untrusted Data, Missing Encryption of Sensitive Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-02

ICSA-21-194-03: **Siemens PROFINET Devices**
High level vulnerability: Allocation of Resources Without Limits or Throttling.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-03

ICSA-21-194-04: **Siemens SINUMERIK Integrate Operate Client**
High level vulnerability: Improper Certificate Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-04

ICSA-21-194-05: **Siemens SIMATIC Software Products**
High level vulnerability: Classic Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-05

ICSA-21-194-06: **Siemens SIMATIC Software Products**
High level vulnerability: Incorrect Permission Assignment for Critical Resource.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-06

ICSA-21-194-07: **Siemens Industrial Products LLDP**
Critical level vulnerabilities: Classic Buffer Overflow, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-07

ICSA-21-194-08: **Siemens Solid Edge**
High level vulnerability: Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-08

ICSA-21-194-09: **Siemens JT Utilities**
Medium level vulnerabilities: Function Call with Incorrect Variable or Reference as Argument, NULL Pointer Dereference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-09

ICSA-21-194-10: **Siemens RUGGEDCOM ROS**
High level vulnerability: Classic Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-10

ICSA-21-194-11: **Siemens Teamcenter Active Workspace**

Medium level vulnerabilities: Generation of Error Message Containing Sensitive Information, Cross-site Scripting, Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-11

ICSA-21-194-12: **Siemens VxWorks-based Industrial Products**

Critical level vulnerability: Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-12

ICSA-21-194-13: **Siemens SINAMICS PERFECT HARMONY GH180**

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-13

ICSA-21-194-14: **Siemens RWG Universal Controllers**

Medium level vulnerability: Allocation of Resources Without Limits or Throttling.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-14

ICSA-21-194-15: **Siemens JT2Go and Teamcenter Visualization**

High level vulnerabilities: Double Free, Infinite Loop, Out-of-bounds Write, Use After Free, Heap-based Buffer Overflow, Buffer Over-read, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-15

ICSA-21-194-16: **Siemens Mendix**

Medium level vulnerability: Incorrect Authorization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-16

ICSA-21-194-17: **Siemens SINUMERIK ONE and SINUMERIK MC**

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-17



ICSA-21-131-03: **Siemens Linux Based Products (Update B)**

High level vulnerability: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-03

ICSA-18-067-01: **Siemens SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet Module (Update D)**

High level vulnerabilities: Missing Authentication for Critical Function, Inadequate Encryption Strength.
https://us-cert.cisa.gov/ics/advisories/ICSA-18-067-01

ICSA-20-196-05: **Siemens UMC Stack (Update H)**

Medium level vulnerabilities: Unquoted Search Path or Element, Uncontrolled Resource Consumption, Improper Input Validation.

https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-19-253-03: **Siemens Industrial Products** (Update N)

High level vulnerabilities: Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03

ICSA-21-189-01: **Rockwell Automation MicroLogix 1100**

High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-189-01

ICSA-21-189-02: **MDT AutoSave**

Critical level vulnerabilities: Inadequate Encryption Strength, SQL Injection, Relative Path Traversal, Command Injection, Uncontrolled Search Path Element, Generation of Error Message Containing Sensitive Information, Unrestricted Upload of File with Dangerous Type.
https://us-cert.cisa.gov/ics/advisories/icsa-21-189-02

ICSA-20-084-01: **VISAM Automation Base (VBASE)** (Update A)

Critical level vulnerabilities: Relative Path Traversal, Incorrect Default Permissions, Inadequate Encryption Strength, Insecure Storage of Sensitive Information, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-20-084-01

ICSMA-21-187-01: **Philips Vue PACS**

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.
https://us-cert.cisa.gov/ics/advisories/icsma-21-187-01

ICSA-21-187-01: **Moxa NPort IAW5000A-I/O Series Serial Device Server**

Critical level vulnerabilities: Classic Buffer Overflow, Stack-based Buffer Overflow, Improper Input Validation, OS Command Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-187-01

ICSA-21-182-01: **Johnson Controls Facility Explorer**

High level vulnerability: Improper Privilege Management.
https://us-cert.cisa.gov/ics/advisories/icsa-21-182-01

ICSA-21-182-02: **Sensormatic Electronics C-CURE 9000**

High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-182-02

ICSA-21-182-03: **Delta Electronics DOPSoft**

High level vulnerability: Out-of-bounds Read.

https://us-cert.cisa.gov/ics/advisories/icsa-21-182-03

ICSA-21-182-04: **Mitsubishi Electric Air Conditioning System**
High level vulnerability: Incorrect Implementation of Authentication Algorithm.
https://us-cert.cisa.gov/ics/advisories/icsa-21-182-04

ICSA-21-182-05: **Mitsubishi Electric Air Conditioning Systems**
Critical level vulnerability: Improper Restriction of XML External Entity Reference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-182-05

ICSA-21-026-01: **All Bachmann M1 System Processor Modules**
High level vulnerability: Use of Password Hash with Insufficient Computational Effort.
https://us-cert.cisa.gov/ics/advisories/icsa-21-026-01-0

ICSA-21-180-01: **Exacq Technologies exacqVision Web Service**
Medium level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-01

ICSA-21-180-02: **Exacq Technologies exacqVision Enterprise Manager**
Law level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-02

ICSA-21-180-03: **Panasonic FPWIN Pro**
Medium level vulnerability: Improper Restriction of XML External Entity Reference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-03

ICSA-21-180-04: **JTEKT TOYOPUC PLC**
Medium level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-04

ICSA-21-180-05: **AVEVA System Platform**
High level vulnerability: Missing Authentication for Critical Function, Uncaught Exception.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-05

ICSA-21-180-06: **Claroty Secure Remote Access Site**
Medium level vulnerability: Authentication Bypass Using an Alternate Path or Channel.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-06

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 July 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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