Key Trends in ICS and Medical Vulnerability Advisories for 2022

Critical Infrastructure (CI) Fusion (FS)

Vulnerability (VU)

January 13, 2023 05:42:53 PM, 23-00000910, Version: 1

Executive Summary

- The Cybersecurity and Infrastructure Security Agency (CISA) maintains the largest public repository specialized in sharing information about industrial control systems (ICS)-specific vulnerability disclosures.
- Organizations in multiple sectors benefit from this platform's information and use it as a component of their vulnerability management processes or to gain situational awareness.
- Mandiant analyzed CISA advisories published in 2022 to identify the top trends in ICS vulnerabilities present in the CISA repository. While the number of vulnerabilities disclosed in 2022 was slightly less than in 2021, we see a general upward trend over time in the number of disclosed vulnerabilities as ICS systems gain more interest from government, industry, and academia.
- Aggregated analysis of public vulnerability advisories is useful to evaluate sources of information, generate statistics to obtain support from executives, identify limitations and opportunities offered by the dataset, and raise awareness about security trends defining the threat landscape.

Threat Detail

The Cybersecurity and Infrastructure Security Agency (CISA), formerly US/ICS-CERT, maintains the largest public repository specialized in sharing information about industrial control systems (ICS)-specific vulnerability disclosures. Organizations in multiple sectors benefit from this platform's information and use it as a component of their vulnerability management processes or to gain situational awareness. While the repository contains a collection of more than 10 years of advisories, limited research exists analyzing this data from an aggregated perspective. Statistics pertaining to ICS vulnerabilities can be leveraged to evaluate sources of information by comparing strengths and limitations of different datasets, generate visual materials for obtaining support from executives, and raise awareness about security trends or promote better understanding of the threat landscape.

Mandiant analyzed 459 CISA advisories published between January and December 2022 to identify the top trends in ICS vulnerability disclosures present in the CISA repository. Of the 459 advisories, 21 were medical advisories covering 80 vulnerabilities.

Summary of ICS Vulnerability Advisories for 2022

According to the data we retrieved from CISA advisories published between January and December 2022, CISA released 459 advisories with information on 1,454 unique vulnerabilities categorized by Common Vulnerability Enumeration (CVE) identifiers. Of the 1,454 vulnerabilities, 767 were assigned CVEs during 2022.

However, not all ICS vulnerability information is necessarily consolidated into the database, so organizations can benefit from consulting multiple information sources when searching for vulnerabilities in their assets. Figure 1 shows the number of vulnerabilities published per year since 2010 (20-00000458, 21-00000587). The annual growth in disclosures is consistent with what we would expect based on increasing interest in cyber physical security among government institutions, industry practitioners, academic researchers, and in media coverage.

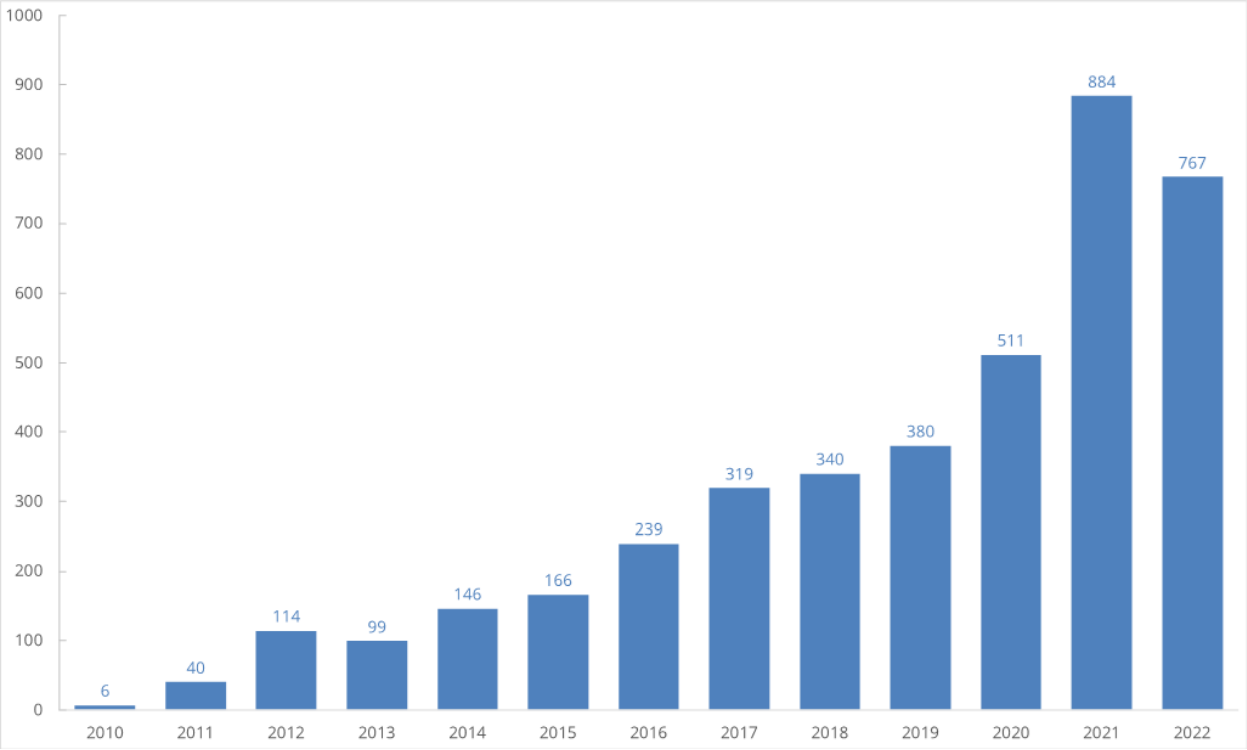

Figure 1: CISA yearly disclosed vulnerabilities between March 2010 and December 2022

Most Vulnerability Disclosures Pertain to Highest-Impact Critical Infrastructure Sectors

These advisories pertain to widely applicable products that can be used in different types of facilities. However, the most frequently mentioned sectors were critical manufacturing, energy, and water/wastewater systems. While good vulnerability management practices should be present in any ICS environment, organizations from heavily affected industries should remain especially aware of known vulnerabilities that may be used to impact their operations. Reported vulnerability information is public and may be leveraged by attackers in the absence of proper mitigations.

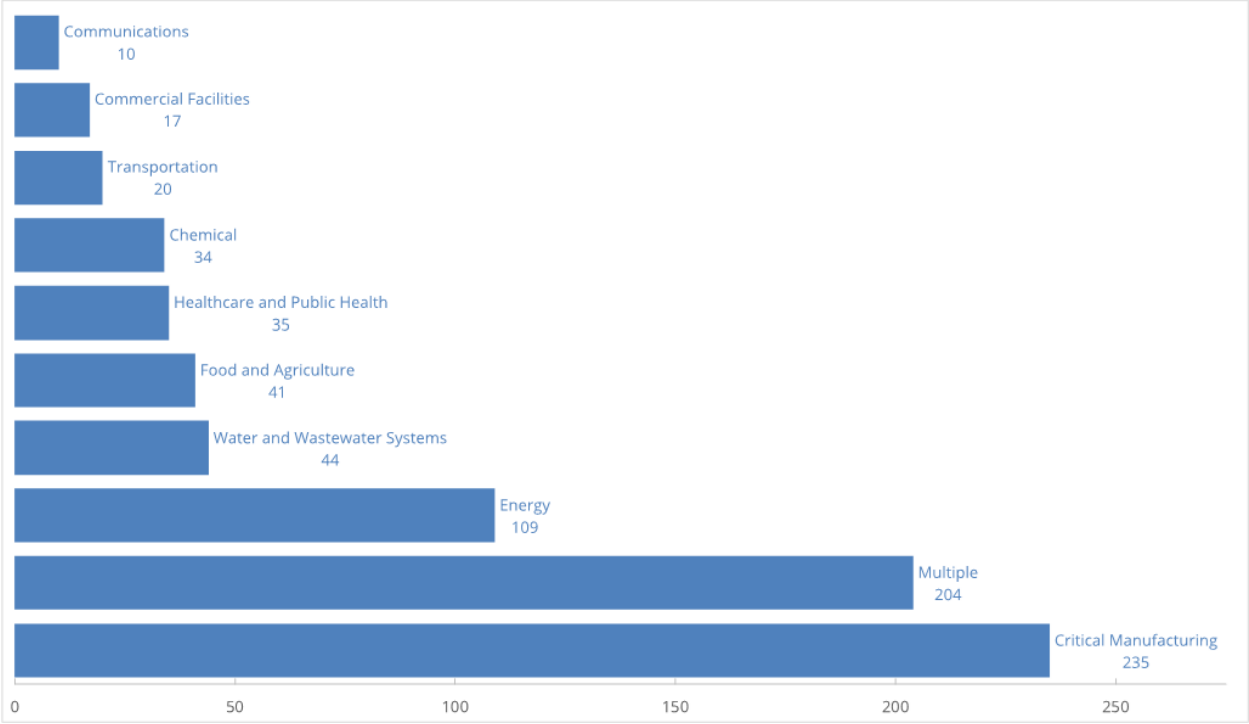

Figure 2: Top 10 affected industries by sector

Most Vulnerabilities Are Disclosed for Major ICS Vendor Products

Eighty-six (86) unique vendors were identified in ICS and ICS Medical Advisories (ICSMA) for 2022. Sixty (60) percent of all advisories were divided among the top 10 vendors. According to the data we retrieved from CISA, top ICS vendors participated in the disclosures. In the case of Siemens, the large increase in vulnerabilities year over year and its position at the top of the vendor list is likely driven by its ProductCERT team, which coordinates vulnerability disclosures from security researchers, industry groups, government organizations, and vendors.

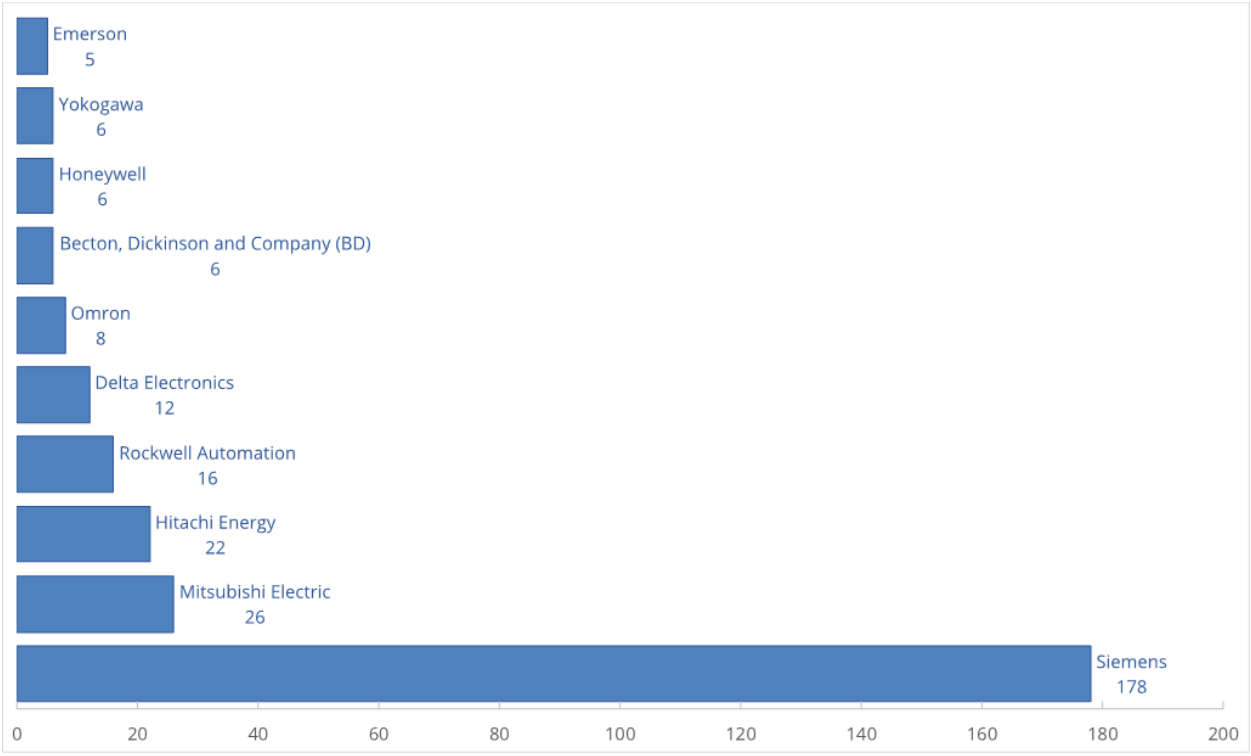

Figure 3: Top 10 vendors for all 2022 CISA advisories

CISA Ranked Majority of Advisories as High-Security Risks

The Common Vulnerability Scoring System (CVSS) is a mechanism that captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Since 2017, CISA has rated its advisories with a unique CVSS value calculated following a process called Vulnerability Chaining. This process attempts to address situations where multiple vulnerabilities are exploited in the course of a single attack to compromise a host or application. As a result, we only extracted a single CVSS score per advisory, regardless of whether multiple vulnerabilities were described in the same document.

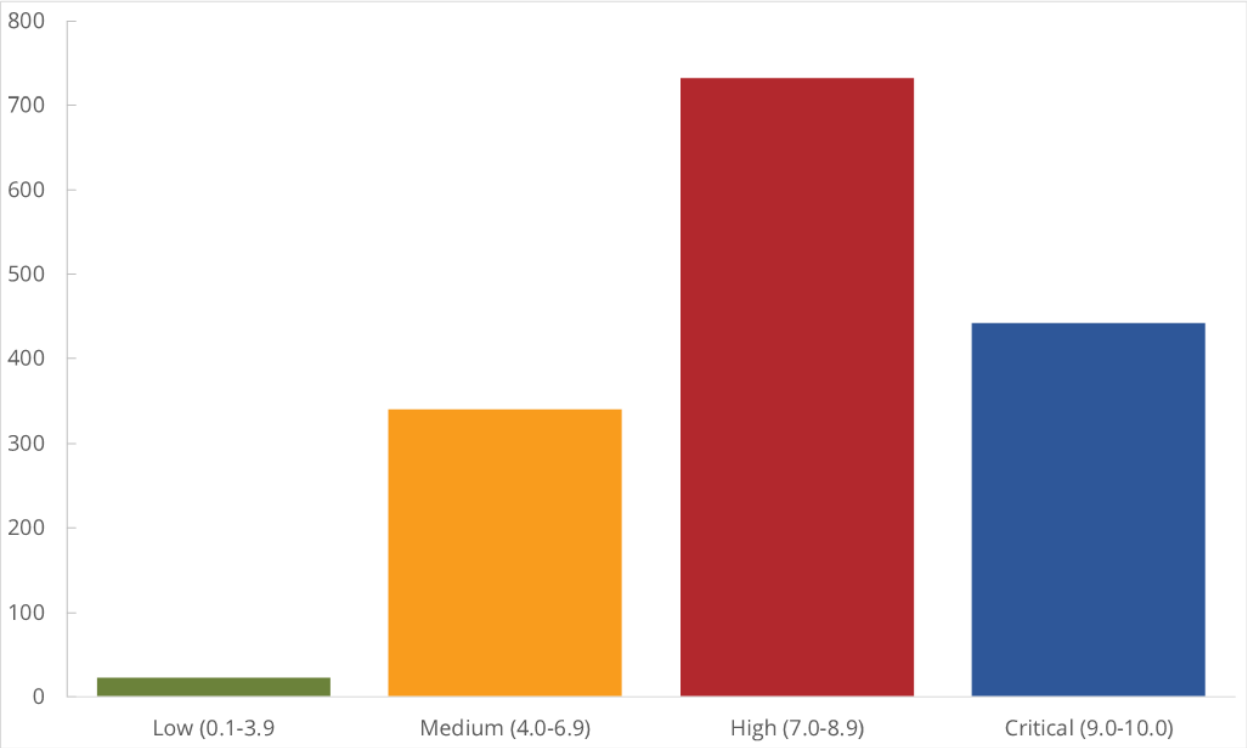

Figure 4: Vulnerabilities by severity

Most Common Types of Vulnerabilities Reported by CISA

Common Weakness Enumeration (CWE) is a standard dictionary developed by MITRE to categorize types of vulnerabilities that have been found in the code of different products. Based on this dictionary, we identified 185 unique types of vulnerabilities in CISA advisories. The top 10 accounted for 40% of all unique vulnerabilities (Figure 5).

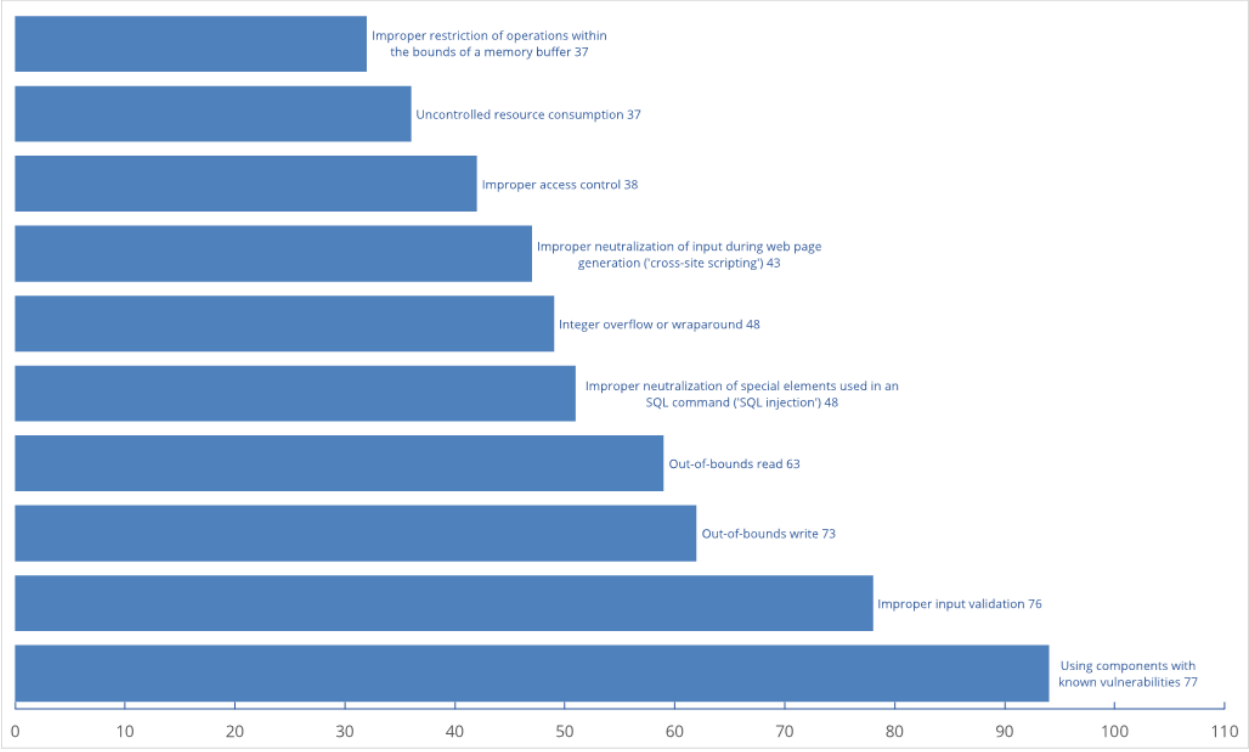

Figure 5: Top 10 types of vulnerabilities reported by CISA

The description for these 10 types of vulnerabilities are as follows.

CWE-1035: Using components with known vulnerabilities – Weaknesses in this category are related to the A9 category in the OWASP Top Ten 2017.

CWE-20: Improper input validation – The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

CWE-787: Out-of-bounds write – The software writes data past the end, or before the beginning, of the intended buffer.

CWE-125: Out-of-bounds read – The software reads data past the end, or before the beginning, of the intended buffer.

CWE-89: Improper neutralization of special elements used in an SQL command ('SQL injection') – The software constructs all or part of a SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

CWE-190: Integer overflow or wraparound – The software performs a calculation that can produce an integer overflow or wraparound when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control.

CWE-79: Improper neutralization of input during webpage generation ('cross-site scripting') – The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a webpage that is served to other users.

CWE-284: Improper access control – The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

CWE-400: Uncontrolled resource consumption – The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the number of resources consumed, eventually leading to the exhaustion of available resources.

CWE-119: Improper restriction of operations within the bounds of a memory buffer – The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.

Learning about the most common types of vulnerabilities in ICS assets is useful for security and incident response practitioners to understand how to identify and mitigate them.

Outlook

While the number of vulnerabilities disclosed in 2022 was slightly less than in 2021, the overall trend over time of increased vulnerability disclosures is consistent with our observations from past years. The large number of vulnerabilities reported by Siemens continues to highlight the value of conducting an internal CERT to facilitate and coordinate disclosure from researchers. As the volume of data that is released about ICS vulnerabilities increases, we expect to see more interest in understanding the trends and finding solutions to handle and categorize this information. For example, this process could include translating ICS vulnerability information into popular markup languages or working on methodologies to assess risk to OT beyond the CVSS.

Appendix A: List of Critical Advisories Published in 2022

Advisory	Vendor	Equipment	Vector	CVSSv3 Score	Industry
ICSA-22-034-01	Sensormatic Electronics, LLC, a subsidiary of Johnson Controls Inc	PowerManage	Exploitable remotely/low attack complexity	10	Critical Manufacturing
ICSA-20-168-01	Treck Inc.	TCP/IP	Exploitable remotely/public exploits are available	10	Energy
ICSA-22-153-01	Carrier LenelS2	HID Mercury access panels sold by LenelS2	Exploitable remotely/low attack complexity	10	Commercial Facilities
ICSA-22-195-12	Siemens	SIMATIC CP Devices	Exploitable remotely/low attack complexity	10	Multiple
ICSA-22-307-01	ETIC Telecom	Remote Access Server (RAS)	Exploitable remotely/low	10	Multiple

			attack complexity		
ICSA-22-130-05	AVEVA	AVEVA InTouch Access Anywhere and AVEVA Plant SCADA Access Anywhere	Exploitable remotely/low attack complexity	9.9	Chemical, Critical Manufacturing, Energy, Food and Agriculture, Water and Wastewater Systems
ICSA-22-006-03	IDEC	PLCs (Programmable Logic Controllers)	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-020-01	ICONICS and Mitsubishi Electric	ICONICS Product Suite, Mitsubishi Electric MC Works64	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSMA-21-355-01	Fresenius Kabi	Agilia Connect Infusion System	Exploitable remotely/low attack complexity	9.8	Healthcare and Public Health
ICSA-21-315-02	Eclipse, eProsima, GurumNetworks, Object Computing, Inc. (OCI), Real-Time Innovations (RTI), TwinOaks Computing	CycloneDDS, FastDDS, GurumDDS, OpenDDS, Connext DDS Professional, Connext DDS Secure, Connext DDS Micro, CoreDX DDS	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-032-02	Advantech	ADAM-3600	Exploitable remotely/low attack complexity	9.8	Energy, Water and Wastewater Systems
ICSA-22-032-01	Ricon Mobile, Inc.	Industrial Cellular Router	Exploitable remotely/low attack complexity/public exploits are available	9.8	Communications
ICSA-22-034-02	Airspan Networks	Mimosa by Airspan product line	Exploitable remotely/low attack complexity	9.8	Communications
ICSA-22-046-01	Schneider Electric	IGSS (Interactive Graphical SCADA System)	Exploitable remotely/low attack complexity	9.8	Commercial Facilities, Critical Manufacturing, Energy
ICSA-22-053-02	GE	Proficy CIMPLICITY	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-055-02	Mitsubishi Electric Corporation	Energy Saving Data Collecting Server (EcoWebServerIII)	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing

ICSA-22-063-01	Power Line Communications	Power Line Communications (PLC): J2497 (aka PLC4TRUCKS)	Exploitable remotely/low attack complexity	9.8	Transportation Systems
ICSA-22-069-04	Siemens	Mendix Forgot Password Appstore module	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-069-09	Siemens	SINEC INS	Exploitable remotely/low attack complexity	9.8	Not Specified
ICSA-20-203-01	Wibu-Systems AG	CodeMeter	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-083-01	Yokogawa	CENTUM and Exaopc	Exploitable remotely/low skill level to exploit	9.8	Critical Manufacturing, Energy, Food and Agriculture
ICSA-22-067-01	PTC	Axeda agent, Axeda Desktop Server	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-090-06	General Electric Renewable Energy	MDS iNET/iNET II/SD/TD220/TD220MAX Radios	Exploitable remotely/low attack complexity	9.8	Communications, Critical Manufacturing, Energy, Healthcare and Public Health, Transportation Systems, Water and Wastewater Systems
ICSA-22-090-05	Rockwell Automation	Logix Controllers	Exploitable remotely/low attack complexity	9.8	Multiple
ICSMA-21-187-01	Philips	Vue PACS	Exploitable remotely/low attack complexity	9.8	Healthcare and Public Health
ICSA-22-097-01	Pepperl+Fuchs	WirelessHART-Gateway	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-102-02	Mitsubishi Electric	MELSEC-Q Series C Controller Module	Exploitable remotely	9.8	Critical Manufacturing
ICSA-22-104-02	Johnson Controls Inc.	Metasys ADS/ADX/OAS Servers	Exploitable remotely	9.8	Critical Manufacturing
ICSA-22-104-03	Red Lion	DA50N	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-	Siemens	SCALANCE X-300	Exploitable	9.8	Multiple

104-09		switch family devices	remotely/low attack complexity		
ICSA-22-104-11	Siemens	SIMATIC Energy Manager	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-069-12	Siemens	RUGGEDCOM ROS	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-21-119-04	Multiple	Multiple	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-109-04	Elcomplus	SmartPTT	Exploitable remotely/low attack complexity	9.8	Communications
ICSA-22-109-05	Elcomplus	SmartPTT SCADA Server	Exploitable remotely/low attack complexity	9.8	Communications
ICSA-22-132-07	Siemens	Siemens SICAM P850 and SICAM P855	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-132-02	Mitsubishi Electric	MELSOFT iQ AppPortal	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-132-04	Cambium Networks	cnMaestro	Exploitable remotely/low attack complexity	9.8	Information Technology
ICSA-21-315-07	Siemens	Nucleus RTOS based APOGEE and TALON Products	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-146-01	Keysight Technologies, Inc.	N6854A Geolocation server and N6841A RF Sensor software	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing, Transportation Systems
ICSA-22-165-03	Mitsubishi Electric	MELSEC-Q/L Series and iQ-R Series	Exploitable remotely	9.8	Critical Manufacturing
ICSA-22-167-17	Siemens	SINEMA Remote Connect Server	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-167-08	Siemens	SICAM GridEdge Essential ARM	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-167-09	Siemens	SCALANCE LPE9403	Exploitable remotely, low attack complexity	9.8	Multiple
ICSA-22-172-06	Siemens	SIMATIC WinCC OA	Exploitable remotely/low attack complexity	9.8	Multiple

ICSA-22-172-04	Phoenix Contact	ProConOS/ProConOS eCLR and MULTIPROG	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-172-05	Phoenix Contact	ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-172-02	JTEKT	TOYOPUC Products	Exploitable remotely	9.8	Critical Manufacturing
ICSA-22-172-03	Phoenix Contact	ILC, AXC, RFC, PC WORX, FC	Exploitable remotely/low attack complexity	9.8	Multiple
ICSMA-22-174-01	OFFIS	DCMTK	Exploitable from an adjacent network/low attack complexity	9.8	Healthcare and Public Health
ICSA-22-174-03	Secheron	SEPCOS Control and Protection Relay	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-179-02	Omron	SYSMAC CS/CJ/CP Series and NJ/NX Series	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-179-06	Motorola Solutions	ACE1000	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-179-05	Motorola Solutions	MDLC	Exploitable remotely	9.8	Multiple
ICSA-22-179-03	Advantech	iView	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-181-01	Exemys	RME1	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-188-02	Bently Nevada	3701/4X series and 60M100 (3701/60) Condition Monitoring System	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-21-315-03	Siemens	SIMATIC WinCC	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-195-01	Siemens	SCALANCE X Switch Devices	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-21-194-12	Siemens	Wind River VxWorks-based Industrial	Exploitable remotely/low	9.8	Multiple

		Products	attack complexity		
ICSA-22-202-04	ICONICS, Mitsubishi Electric	ICONICS Product Suite, MC Works64	Low attack complexity	9.8	Critical Manufacturing
ICSA-22-207-02	Honeywell	Safety Manager	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-081-01	Delta Electronics	DIAEnergie	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-21-238-03	Delta Electronics	DIAEnergie	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-207-01	Inductive Automation	Ignition	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing, Energy, Information Technology
ICSA-22-216-01	Digi International, Inc.	ConnectPort X2D Gateway	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-223-04	Emerson	ROC800, ROC800L and DL8000	High attack complexity	9.8	Multiple
ICSA-22-223-03	Schneider Electric	EcoStruxure, EcoStruxure Process Expert, SCADAPack RemoteConnect for x70	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-223-02	Siemens	Teamcenter	Exploitable remotely/low attack complexity	9.8	Multiple
ICSMA-20-170-04	Baxter	Sigma Spectrum Infusion Pumps	Exploitable remotely/low attack complexity	9.8	Healthcare and Public Health
ICSA-22-228-04	Softing	Secure Integration Server	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-228-05	B&R Industrial Automation	Automation Studio 4	Exploitable remotely	9.8	Chemical, Critical Manufacturing, Energy
ICSA-22-228-07	Sequi	Sequi PortBloque S	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-21-194-07	Siemens	Industrial Products	Exploitable remotely/low attack complexity	9.8	Chemical, Critical Manufacturing, Energy, Food and Agriculture

ICSA-22-153-02	Illumina	Local Run Manager (LRM)	Exploitable remotely/low attack complexity	9.8	Healthcare and Public Health
ICSA-22-242-11	Sensormatic Electronics, a subsidiary of Johnson Controls Inc.	iSTAR Ultra	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-242-06	Honeywell	ControlEdge	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-242-03	Hitachi Energy	MSM Product	Exploitable remotely/low attack complexity	9.8	Energy
ICSA-22-249-03	Cognex	3D-A1000 Dimensioning System	Exploitable remotely, low attack complexity	9.8	Commercial Facilities, Transportation
ICSA-22-251-01	MZ Automation GmbH	libIEC61850	Exploitable remotely/low attack complexity	9.8	Energy
ICSA-22-256-03	Delta Electronics	DIAEnergie	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-20-324-02	Paradox	IP150	Exploitable remotely/low skill level to exploit	9.8	Multiple
ICSA-22-263-02	Hitachi Energy	AFF660/665 Firewall	Exploitable remotely/low attack complexity	9.8	Energy
ICSA-22-263-03	Dataprobe	iBoot-PDU FW	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-200-01	MiCODUS	MV720 GPS tracker	Exploitable remotely/low attack complexity	9.8	Transportation Systems, Government Facilities, Financial Services, Critical Manufacturing
ICSA-20-245-01	Mitsubishi Electric	Multiple Products	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-20-212-02	Mitsubishi Electric	Mitsubishi Electric, Multiple Factory Automation Engineering Software products	Exploitable remotely	9.8	Critical Manufacturing
ICSA-22-	Rockwell	ThinManager	Exploitable	9.8	Critical

270-03	Automation	ThinServer	remotely		Manufacturing
ICSA-22-270-01	Hitachi Energy	AFS660/AFS665	Exploitable remotely/low attack complexity	9.8	Energy
ICSA-22-284-02	Daikin Holdings Singapore Pte Ltd.	SVMPC1, SVMPC2	Exploitable remotely/low attack complexity	9.8	Energy
ICSA-22-286-13	Siemens	LOGO! 8 BM Devices	Exploitable remotely/low attack complexity	9.8	Chemical, Energy, Food and Agriculture, Water and Wastewater Systems
ICSA-22-286-16	Siemens	Desigo CC and Cerberus DMS	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-167-06	Siemens	Apache HTTP Server	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-286-05	Hitachi Energy	Lumada Asset Performance Manager (APM)	Exploitable remotely/public exploits are available	9.8	Energy
ICSA-21-287-07	Siemens	SCALANCE	Exploitable remotely/low attack complexity	9.8	Chemical, Energy, Food and Agriculture, Healthcare and Public Health, Transportation Systems, Water and Wastewater Systems
ICSA-21-315-06	Siemens	SCALANCE W1750D	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-291-01	Advantech	R-SeeNet	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing, Energy, Water and Wastewater Systems
ICSMA-21-294-01	B. Braun Melsungen AG	Infusomat Space Large Volume Pump	Exploitable remotely/low attack complexity	9.8	Healthcare and Public Health
ICSA-22-298-07	Delta Electronics	InfraSuite Device Master	Exploitable remotely/low attack complexity	9.8	Energy
ICSA-22-298-03	Siemens	Siveillance Video 2022 R2	Exploitable remotely/low	9.8	Communications, Commercial

			attack complexity		Facilities
ICSA-22-298-02	HEIDENHAIN	HEIDENHAIN TNC 640 controlling a HARTFORD 5A-65E CNC machine	Exploitable remotely	9.8	Multiple
ICSA-22-221-01	Mitsubishi Electric	GOT2000 compatible HMI software, CC-Link IE TSN Industrial Managed Switch, MELSEC iQ-R Series OPC UA Server Module	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-258-04	Siemens	Mendix SAML Module	Exploitable remotely	9.8	Multiple
ICSA-21-350-06	Siemens	Capital VSTAR	Exploitable remotely / Low attack complexity	9.8	Critical Manufacturing
ICSA-22-314-10	Siemens	SCALANCE W1750D	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-319-01	Mitsubishi Electric Corporation	GT SoftGOT2000	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSMA-21-152-01	Hillrom	Welch Allyn medical device management tools	Exploitable remotely	9.8	Healthcare and Public Health
ICSA-20-212-04	Mitsubishi Electric	Mitsubishi Electric, Factory Automation Engineering products	Exploitable remotely	9.8	Critical Manufacturing
ICSA-21-049-02	Mitsubishi Electric	FA Engineering Software Products	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-19-346-02	Omron	PLC CJ and CS Series	Exploitable remotely/low skill level to exploit	9.8	Critical Manufacturing
ICSA-22-335-02	Horner Automation	Remote Compact Controller (RCC) 972	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-347-03	Contec	CONPROSYS HMI System (CHS)	Exploitable remotely/low attack complexity	9.8	Multiple
ICSA-22-349-21	Siemens	SCALANCE X-200RNA switch devices before V3.2.7	Exploitable remotely/low attack complexity/public exploits are available	9.8	Multiple
ICSA-22-	Siemens	SICAM PAS	Exploitable	9.8	Energy

349-19			remotely/low attack complexity		
ICSA-22-349-04	Siemens	RUGGEDCOM and SCALANCE devices	Exploitable remotely/low attack complexity	9.8	Critical Manufacturing
ICSA-22-349-02	Siemens	SCALANCE	Exploitable remotely/low attack complexity/public exploits available	9.8	Chemical, Critical Manufacturing, Energy, Food and Agriculture, Water and Wastewater Systems
ICSA-22-300-02	SAUTER Controls	moduWeb	Exploitable remotely/low attack complexity	9.6	Critical Manufacturing, Energy
ICSA-22-013-03	Siemens Energy	PLUSCONTROL	Exploitable remotely/low attack complexity	9.1	Multiple
ICSA-22-069-02	Siemens	SIMOTICS CONNECT 400	Exploitable remotely/low attack complexity	9.1	Energy
ICSA-22-111-02	Johnson Controls, Inc.	Metasys	Exploitable remotely/low attack complexity	9.1	Critical Manufacturing
ICSA-22-123-01	Yokogawa	CENTUM and ProSafe-RS	Exploitable remotely/low attack complexity	9.1	Critical Manufacturing, Energy, Food and Agriculture
ICSA-22-090-04	Mitsubishi Electric	FA products	Exploitable remotely	9.1	Critical Manufacturing
ICSA-22-132-10	Siemens	PXC and DXR Devices	Exploitable remotely/low attack complexity	9.1	Multiple
ICSA-22-181-04	Distributed Data Systems	WebHMI	Exploitable remotely/low attack complexity/public exploits are available	9.1	Commercial Facilities, Critical Manufacturing, Food and Agriculture, Water and Wastewater Systems
ICSA-19-085-01	Siemens	SCALANCE X	Exploitable remotely	9.1	Chemical, Critical Manufacturing, Energy, Food and Agriculture, Water and Wastewater Systems
ICSA-22-195-15	Siemens	SIMATIC eaSie	Exploitable remotely/low	9.1	Critical Manufacturing

			attack complexity		
ICSA-22-242-05	Fuji Electric	D300win	Exploitable remotely/low attack complexity	9.1	Multiple
ICSA-22-242-07	Honeywell	Experion LX	Exploitable remotely/low attack complexity	9.1	Multiple
ICSA-22-256-04	Kingspan	TMS300 CS	Exploitable remotely/Low attack complexity	9.1	Water and Wastewater Systems
ICSA-22-167-02	AutomationDirect	DirectLOGIC with Serial Communication	Low attack complexity	9.1	Multiple
ICSA-22-167-03	AutomationDirect	DirectLOGIC with Ethernet Communication Modules	Exploitable remotely/low attack complexity	9.1	Multiple
ICSA-21-250-01	Mitsubishi Electric Corporation	MELSEC iQ-R Series CPU Module	Exploitable remotely	9.1	Critical Manufacturing
ICSA-22-314-06	Siemens	QMS Automotive	Exploitable remotely/low attack complexity	9.1	Critical Manufacturing
ICSA-22-333-05	Mitsubishi Electric	GX Works3, MX OPC UA Module Configurator-R	Exploitable remotely/low attack complexity	9.1	Critical Manufacturing
ICSA-22-174-05	Elcomplus LLC	SmartICS	Exploitable remotely/low attack complexity	9	Communications, Commercial Facilities, Energy, Water and Wastewater Systems

Table 1: List of critical advisories published in 2022

Please rate this product by taking a short four question survey

First Version Publish Date

January 13, 2023 05:42:53 PM

Threat Intelligence Tags

Affected Industries

- Aerospace & Defense
- Automotive
- Chemicals & Materials
- Construction & Engineering
- Energy & Utilities
- Healthcare
- Manufacturing

- Oil & Gas
- Telecommunications
- Transportation

Affected Systems

- Third Party Services
- Users/Application and Software
- Equipment Under Control
- Industrial Network Protocols
- Industrial Internet of Things
- Operations Management

Intended Effects

- Disruption
- Interference with ICS
- Degradation

Tactics, Techniques And Procedures (TTPs)

- Exploit Development
- Malware Research and Development
- Malware Propagation and Deployment

Version Information

Version:1, January 13, 2023 05:42:53 PM

german[.]simkin@mandiant.com