Industrial Control Systems and Medical Vulnerability Advisories Reported by CISA in November 2022

Critical Infrastructure (CI) | Fusion (FS)

Vulnerability (VU)

December 1, 2022 01:08:19 PM, 22-00026583, Version: 1

Executive Summary

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) maintains the largest public repository specialized in sharing information about industrial control systems (ICS) and medical device-specific vulnerability disclosures.
- In November 2022, CISA published 42 advisories related to vulnerabilities in ICS or medical devices.
- The advisories presented information on 112 Common Vulnerability Enumeration (CVE) IDs from which 19 received a critical Common Vulnerability Scoring System (CVSSv3) score of 9 or higher.

Threat Detail

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) continues to maintain the largest public repository specialized in sharing information about industrial control systems (ICS) and medical device-specific vulnerability disclosures. Organizations relying on cyber physical assets such as operational technologies (OT) can benefit from this information and use it as a component of vulnerability management processes or to gain situational awareness. In this document we present a summary of vulnerabilities reported by CISA during November 2022.

ICS and Medical Vulnerability Disclosure

Mandiant Threat Intelligence extracted all Common Vulnerability Enumeration (CVE) IDs when available from advisories and identified 112 unique values. We include new CVEs and those that were updated to disclose additional information. The most commonly seen CWEs (Common Weakness Enumerations) as reported by CISA were:

- CWE-79: CROSS-SITE SCRIPTING
  - A vulnerability in the web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.
- CWE-20: IMPROPER INPUT VALIDATION
  - An unauthenticated denial of service (DoS) vulnerability exists in the handling of certain SSID strings. Successful exploitation of this vulnerability could result in the ability to interrupt the normal operation of the affected Access Point.

- CWE-89: IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN SQL COMMAND ('SQL INJECTION')
    - The affected product DIAEnergie (versions prior to v1[.]9[.]01[.]002) is vulnerable to a SQL injection that exists in CheckIoTHubNameExisted. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries.
- CWE-120: CLASSIC BUFFER OVERFLOW
    - A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211).
- CWE-125: OUT-OF-BOUNDS READ
    - Siemens Parasolid contains an out-of-bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.

Of all the advisories, 11 received a CVSSv3 score of 9 (critical) or higher.

- ICS Advisory (ICSA-22-307-01)
    - ETIC Telecom Remote Access Server (RAS)
- ICS Advisory (ICSA-22-221-01)
    - Mitsubishi Electric Multiple Factory Automation Products (Update C)
- ICS Advisory (ICSA-22-314-04)
    - Siemens SINUMERIK ONE and SINUMERIK MC
- ICS Advisory (ICSA-22-314-08)
    - Omron NJ/NX-series Machine Automation Controllers
- ICS Advisory (ICSA-22-314-10)
    - Siemens SCALANCE W1750D
- ICS Advisory (ICSA-22-314-11)
    - Siemens SICAM Q100
- ICS Advisory (ICSA-22-286-15)
    - Siemens SCALANCE X-200 and X-200IRT Families (Update A)
- ICS Advisory (ICSA-21-350-13)
    - Siemens Questa and ModelSim (Update A)
- ICS Advisory (ICSA-22-319-01)
    - Mitsubishi Electric GT SoftGOT2000
- ICS Advisory (ICSA-22-326-01)
    - AVEVA Edge
- ICS Advisory (ICSA-22-333-05)
    - Mitsubishi Electric FA Engineering Software

Disclosed Vulnerabilities by Vendor

The following figure shows the number of CVEs that were published in CISA advisories during the month, categorized by vendor and severity level. The vendors are ordered by the total number of vulnerabilities reported.

Vendor	Low	Medium	High	Critical
Siemens		11	22	13
Mitsubishi Electric	1	7	9	2
Delta Electronics			13	
Omron		1	4	1
GE			5	
AVEVA		1	2	1
ETIC Telecom			2	1
Nokia			3	
Phoenix Contact			2	
Moxa			2	
Hitachi Energy			2	
Mitsubishi Electric Corporation				1
Digital Alert Systems		2		
Hillrom		2		
Delta Industrial Automation			1	
Red Lion Controls			1	
Cradlepoint			1	
LS ELECTRIC, LS Industrial Systems (LSIS) Co. Ltd		1		

Figure 1: CVE count by vendor

ICS and Medical Vulnerable Products as Reported in November 2022 by CISA

The following table contains a compilation of CVEs reported by CISA for the month of November 2022. Given the structure of CISA advisories, some CVEs may be duplicated if they were seen in multiple advisories.

Advisory	Vendor	Equipment	CVE(s)
ICS Advisory (ICSA-22-307-01)	ETIC Telecom	Remote Access Server (RAS)	CVE-2022-3703, CVE-2022-41607, CVE-2022-40981
ICS Advisory (ICSA-22-307-02)	Nokia	ASIK AirScale 5G Common System Module	CVE-2022-2482, CVE-2022-2484, CVE-2022-2483
ICS Advisory (ICSA-22-307-03)	Delta Industrial Automation	DIALink	CVE-2022-2969
ICS Advisory	Mitsubishi Electric	GOT2000 compatible HMI software, CC-Link IE TSN	CVE-2022-0778, CVE-2022-1292

(ICSA-22-221-01)		Industrial Managed Switch, MELSEC iQ-R Series OPC UA Server Module	
ICS Advisory (ICSA-22-314-03)	Siemens	SINEC NMS	CVE-2021-42550
ICS Advisory (ICSA-22-314-01)	Siemens	Parasolid	CVE-2022-39157, CVE-2022-43397
ICS Advisory (ICSA-22-314-02)	Siemens	SIMATIC Industrial Controllers and Software	CVE-2022-30694
ICS Advisory (ICSA-22-314-04)	Siemens	SINUMERIK ONE and SINUMERIK MC	CVE-2022-38465
ICS Advisory (ICSA-22-314-05)	Siemens	RUGGEDCOM ROS	CVE-2022-39158
ICS Advisory (ICSA-22-314-06)	Siemens	QMS Automotive	CVE-2022-43958
ICS Advisory (ICSA-22-314-07)	Omron	NJ/NX-series Machine Automation Controllers	CVE-2022-33971
ICS	Omron	NJ/NX-series Controllers	CVE-2022-34151, CVE-2022-33208

Advisory (ICSA-22-314-08)		and Software	
ICS Advisory (ICSA-22-314-09)	Siemens	Teamcenter Visualization and JT2Go	CVE-2022-39136, CVE-2022-41660, CVE-2022-41661, CVE-2022-41662, CVE-2022-41663, CVE-2022-41664
ICS Advisory (ICSA-22-314-10)	Siemens	SCALANCE W1750D	CVE-2002-20001, CVE-2022-37885, CVE-2022-37886, CVE-2022-37887, CVE-2022-37888, CVE-2022-37889, CVE-2022-37890, CVE-2022-37891, CVE-2022-37892, CVE-2022-37896, CVE-2022-37893, CVE-2022-37894, CVE-2022-37895
ICS Advisory (ICSA-22-314-11)	Siemens	SICAM Q100	CVE-2022-43398, CVE-2022-43439, CVE-2022-43545, CVE-2022-43546
ICS Advisory (ICSA-21-350-06)	Siemens	Capital VSTAR	CVE-2021-31344, CVE-2021-31345, CVE-2021-31346, CVE-2021-31881, CVE-2021-31882, CVE-2021-31883, CVE-2021-31884, CVE-2021-31889, CVE-2021-31890
ICS Advisory (ICSA-22-286-15)	Siemens	SCALANCE X-200 and X-200IRT Families	CVE-2022-40631
ICS Advisory (ICSA-22-258-03)	Siemens	RUGGEDCOM ROS	CVE-2022-39158
ICS Advisory (ICSA-22-228-02)	LS ELECTRIC, LS Industrial Systems	LS ELEC PLC and XG5000	CVE-2022-2758

	(LSIS) Co. Ltd		
ICS Advisory (ICSA-22-298-06)	Delta Electronics	DIAEnergie	CVE-2022-41701, CVE-2022-40965, CVE-2022-41555, CVE-2022-41702, CVE-2022-41651, CVE-2022-40967, CVE-2022-41133, CVE-2022-41773, CVE-2022-41775, CVE-2022-43447, CVE-2022-43506, CVE-2022-43457, CVE-2022-43452
ICS Advisory (ICSA-22-258-04)	Siemens	Mendix SAML Module	CVE-2022-37011, CVE-2022-44457
ICS Advisory (ICSA-22-286-11)	Siemens	Multiple SCALANCE and RUGGEDCOM products	CVE-2022-31765
ICS Advisory (ICSA-21-350-13)	Siemens	Questa Simulation and ModelSim Simulation	CVE-2021-42023
ICS Advisory (ICSA-22-069-01)	Siemens	RUGGEDCOM Devices	CVE-2021-37209
ICS Advisory (ICSA-22-321-01)	Red Lion Controls	Crimson	CVE-2022-3090
ICS Advisory (ICSA-22-321-02)	Cradlepoint	IBR600	CVE-2022-3086
ICS Advisory (ICSA-	Mitsubishi Electric Corporation	GT SoftGOT2000	CVE-2022-2068

22-319-01)			
ICS Advisory (ICSA-22-326-01)	AVEVA	Edge	CVE-2016-2542, CVE-2021-42794, CVE-2021-42796, CVE-2021-42797
ICS Advisory (ICSA-22-326-02)	Digital Alert Systems	DASDEC	CVE-2019-18265, CVE-2022-40204
ICS Advisory (ICSA-22-326-03)	Phoenix Contact	Automation Worx Software Suite	CVE-2022-3461, CVE-2022-3737
ICS Advisory (ICSA-22-326-04)	GE	CIMPLICITY	CVE-2022-3084, CVE-2022-2952, CVE-2022-2948, CVE-2022-2002, CVE-2022-3092
ICS Advisory (ICSA-22-326-05)	Moxa	ARM-Based Computers	CVE-2022-3088
ICS Advisory (ICSA-21-049-02)	Mitsubishi Electric	FA Engineering Software Products	CVE-2021-20587, CVE-2021-20588
ICS Advisory (ICSA-20-212-04)	Mitsubishi Electric	Mitsubishi Electric, Factory Automation Engineering products	CVE-2020-14521
ICS Medical Advisory	Hillrom	Welch Allyn medical device management tools	CVE-2021-27410, CVE-2021-27408

(ICSMA-21-152-01)			
ICS Advisory (ICSA-22-333-01)	Mitsubishi Electric	GOT2000 Series	CVE-2022-40266
ICS Advisory (ICSA-22-333-02)	Hitachi Energy	PCM600	CVE-2022-2513
ICS Advisory (ICSA-22-333-03)	Hitachi Energy	MicroSCADA X SYS600, MicroSCADA Pro	CVE-2022-3388
ICS Advisory (ICSA-22-333-04)	Moxa	UC Series	CVE-2022-3086
ICS Advisory (ICSA-22-333-05)	Mitsubishi Electric	GX Works3, MX OPC UA Module Configurator-R	CVE-2022-25164, CVE-2022-29826, CVE-2022-29825, CVE-2022-29831, CVE-2022-29833, CVE-2022-29827, CVE-2022-29828, CVE-2022-29829, CVE-2022-29830, CVE-2022-29832
ICS Advisory (ICSA-21-334-02)	Mitsubishi Electric	MELSEC and MELIPC Series	CVE-2021-20609, CVE-2021-20610, CVE-2021-20611
ICS Advisory (ICSA-19-346-02)	Omron	PLC CJ and CS Series	CVE-2019-18259, CVE-2019-13533, CVE-2019-18269

Table 1: CISA advisories for November 2022

Please rate this product by taking a short four question survey

First Version Publish Date

December 1, 2022 01:08:19 PM

Threat Intelligence Tags

Affected Industries

- Aerospace & Defense
- Automotive
- Chemicals & Materials
- Construction & Engineering
- Energy & Utilities
- Healthcare
- High Tech/Software/Hardware/Services
- Manufacturing
- Oil & Gas
- Pharmaceuticals
- Technology
- Telecommunications
- Transportation

Affected Systems

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

Intended Effects

- Degradation
- Disruption
- Interference with ICS

Tactics, Techniques And Procedures (TTPs)

- Exploit Development
- Malware Research and Development

Version Information

Version:1, December 1, 2022 01:08:19 PM

Common Vulnerabilities and Exposures

CVE ID:	CVE-2021-31883(CVE Description)Mandiant Vulnerability Analysis CVE-2022-3388(CVE Description)Mandiant Vulnerability Analysis CVE-2022-37891(CVE Description)Mandiant Vulnerability Analysis

CVE-2022-37889(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37890(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2948(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43545(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3084(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31345(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-18265(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37895(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3703(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2483(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-27408(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31346(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-27410(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37896(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1292(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43506(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-33208(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29831(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41555(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-44457(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29832(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37892(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2068(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-31765(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2969(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31882(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3737(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29829(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43546(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-38465(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-20588(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-13533(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-20610(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41662(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31890(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37011(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40981(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43397(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43457(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31881(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41702(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41661(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41133(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41607(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41773(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-33971(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-34151(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31889(CVE Description)Mandiant Vulnerability Analysis
CVE-2016-2542(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3092(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-37209(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42794(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43958(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37893(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2513(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-39136(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2482(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42023(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-18259(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41651(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43452(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31344(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40266(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3461(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-25164(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37894(CVE Description)Mandiant Vulnerability Analysis

CVE-2021-20587(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-30694(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40965(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-0778(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43398(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29827(CVE Description)Mandiant Vulnerability Analysis
CVE-2002-20001(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29825(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29828(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3086(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-31884(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43439(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-18269(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37885(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-39158(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-20611(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40631(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-20609(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41775(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29826(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41660(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43447(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40204(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41701(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2002(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2484(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2758(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3088(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40967(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37887(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3090(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41664(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37888(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41663(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42550(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29833(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-39157(CVE Description)Mandiant Vulnerability Analysis
CVE-2020-14521(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29830(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-37886(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2952(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42797(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42796(CVE Description)Mandiant Vulnerability Analysis