Industrial Control Systems and Medical Vulnerability Advisories Reported by CISA in April 2023

Critical Infrastructure (CI) | Fusion (FS)

Vulnerability (VU)

May 1, 2023 12:29:07 PM, 23-00007137, 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 April 2023, CISA published 24 advisories related to vulnerabilities in ICS or medical devices.
- The advisories presented information on 65 Common Vulnerability Enumeration (CVE) IDs from which 17 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 April 2023.

ICS and Medical Vulnerability Disclosure

Mandiant Threat Intelligence extracted all Common Vulnerability Enumeration (CVE) IDs when available from advisories and identified 65 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-125: OUT-OF-BOUNDS READ
  - An out-of-bounds read may occur when processing template information because the end of data cannot be verified.
- CWE-78: OS COMMAND INJECTION
  - mySCADA myPRO versions 8.26.0 and prior has parameters which an authenticated user could exploit to inject arbitrary operating system commands.
- CWE-416: USE AFTER FREE
  - When an error is detected, an out-of-bounds write may occur because there is no error handling process.

- CWE-770: ALLOCATION OF RESOURCES WITHOUT LIMITS OR THROTTLING
    - The webserver of the affected products contains a vulnerability that may lead to a denial-of-service condition. An attacker could cause a denial-of-service condition of the webserver of the affected product.
- CWE-787: OUT-OF-BOUNDS WRITE
    - When an out-of-specification error is detected, an out-of-bounds write may occur because there is no error handling process.

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

- Nexx Smart Home Device | CISA
    -
- Industrial Control Links ScadaFlex II SCADA Controllers | CISA
    -
- Hitachi Energy MicroSCADA System Data Manager SDM600 | CISA
    -
- mySCADA myPRO | CISA
    -
- Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families BadAlloc Vulnerabilities | CISA
    -
- Siemens SCALANCE XCM332 | CISA
    -
- Siemens CPCI85 Firmware of SICAM A8000 Devices | CISA
    -
- Schneider Electric Easy UPS Online Monitoring Software | CISA
    -
- INEA ME RTU | CISA
    -
- Keysight N8844A Data Analytics Web Service | CISA
    -
- Illumina Universal Copy Service | CISA
    -

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		4	11	4
JTEKT ELECTRONICS CORPORATION			10	
mySCADA Technologies				5
Nexx		1	3	1
Hitachi Energy		1	3	1
Schneider Electric			1	2
Korenix		1	2	
Datakit	4		1	
Illumina			1	1
Industrial Control Links				1
INEA				1
Keysight				1
Mitsubishi Electric India			1	
Omron			1	
FANUC		1		
Siemens ProductCERT		1		
Scada-LTS		1		

Figure 1: CVE count by vendor

ICS and Medical Vulnerable Products as Reported in April 2023 by CISA

The following table contains a compilation of CVEs reported by CISA for the month of April 2023. Given the structure of CISA advisories, some CVEs may be duplicated if they were seen in multiple advisories.

Advisory	Vendor	Equipment	CVE(s)
Nexx Smart Home Device | CISA	Nexx	Garage Door Controller, Smart Plug, Smart Alarm	CVE-2023-1748, CVE-2023-1749, CVE-2023-1750, CVE-2023-1751, CVE-2023-1752
Industrial Control Links ScadaFlex II SCADA Controllers | CISA	Industrial Control Links	ScadaFlex II SCADA Controllers	CVE-2022-25359
JTEKT ELECTRONICS Screen Creator Advance 2 | CISA	JTEKT ELECTRONICS CORPORATION	Screen Creator Advance 2	CVE-2023-22345, CVE-2023-22346, CVE-2023-22347, CVE-2023-22349, CVE-2023-22350, CVE-2023-22353, CVE-2023-22360
JTEKT ELECTRONICS Kostac PLC Programming Software | CISA	JTEKT ELECTRONICS CORPORATION	Kostac PLC Programming Software	CVE-2023-22419, CVE-2023-22421, CVE-2023-22424
Korenix Jetwave | CISA	Korenix	Jetwave	CVE-2023-23294, CVE-2023-23295, CVE-2023-23296
Hitachi Energy	Hitachi Energy	MicroSCADA System	CVE-2022-3682, CVE-2022-3683, CVE-

MicroSCADA System Data Manager SDM600 | CISA		Data Manager SDM600	2022-3684, CVE-2022-3685, CVE-2022-3686
mySCADA myPRO | CISA	mySCADA Technologies	mySCADA myPRO	CVE-2023-28400, CVE-2023-28716, CVE-2023-28384, CVE-2023-29169, CVE-2023-29150
FANUC ROBOGUIDE-HandlingPRO | CISA	FANUC	ROBOGUIDE-HandlingPRO	CVE-2023-1864
Mitsubishi Electric India GC-ENET-COM | CISA	Mitsubishi Electric India	GC-ENET-COM	CVE-2023-1285
Datakit CrossCAD/Ware | CISA	Datakit	CrossCAD/Ware_x64 library	CVE-2023-22295, CVE-2023-22321, CVE-2023-22354, CVE-2023-22846, CVE-2023-23579
Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families BadAlloc Vulnerabilities | CISA	Siemens	SCALANCE X-200, X-200IRT, and X-300 Switch Families	CVE-2020-28895, CVE-2020-35198
Siemens Polarion ALM | CISA	Siemens	Polarion ALM	CVE-2023-28828
Siemens Teamcenter Visualization and JT2Go | CISA	Siemens	Teamcenter Visualization and JT2Go	CVE-2023-1709
Siemens Industrial Products | CISA	Siemens	Industrial Products	CVE-2022-43716, CVE-2022-43767, CVE-2022-43768
Siemens SCALANCE XCM332 | CISA	Siemens	SCALANCE XCM332	CVE-2021-46828, CVE-2022-1652, CVE-2022-1729, CVE-2022-30065, CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-35252, CVE-2022-40674
Siemens Mendix Forgot Password Module | CISA	Siemens ProductCERT	Mendix Forgot Password Module	CVE-2023-27464
Siemens CPCI85 Firmware of SICAM A8000 Devices | CISA	Siemens	CPCI85 Firmware of SICAM A8000 Devices	CVE-2023-28489
Siemens SIPROTEC 5 Devices | CISA	Siemens	SIPROTEC 5 Devices	CVE-2023-28766
Schneider Electric Easy	Schneider	APC Easy UPS Online	CVE-2023-29411, CVE-2023-29412,

UPS Online Monitoring Software | CISA	Electric	Monitoring Software, Schneider Electric Easy UPS Online Monitoring Software	CVE-2023-29413
Omron CS/CJ Series | CISA	Omron	SYSMAC CS/CJ Series	CVE-2022-45794
INEA ME RTU | CISA	INEA	ME RTU	CVE-2023-2131
Scada-LTS Third Party Component | CISA	Scada-LTS	Scada-LTS	CVE-2015-1179
Keysight N8844A Data Analytics Web Service | CISA	Keysight	N8844A Data Analytics Web Service	CVE-2023-1967
Illumina Universal Copy Service | CISA	Illumina	Universal Copy Service (UCS)	CVE-2023-1968, CVE-2023-1966

Table 1: CISA advisories for April 2023

First Version Publish Date

May 1, 2023 12:29:07 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, May 1, 2023 12:29:07 PM

Common Vulnerabilities and Exposures

CVE ID:	CVE-2023-23579(CVE Description)Mandiant Vulnerability Analysis CVE-2022-45794(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1968(CVE Description)Mandiant Vulnerability Analysis CVE-2022-25359(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22349(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22846(CVE Description)Mandiant Vulnerability Analysis CVE-2020-35198(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1864(CVE Description)Mandiant Vulnerability Analysis CVE-2022-43716(CVE Description)Mandiant Vulnerability Analysis CVE-2022-35252(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1748(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1967(CVE Description)Mandiant Vulnerability Analysis CVE-2023-23295(CVE Description)Mandiant Vulnerability Analysis CVE-2023-29150(CVE Description)Mandiant Vulnerability Analysis CVE-2023-28489(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1966(CVE Description)Mandiant Vulnerability Analysis CVE-2022-1652(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1752(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22360(CVE Description)Mandiant Vulnerability Analysis CVE-2022-3682(CVE Description)Mandiant Vulnerability Analysis CVE-2022-3684(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1709(CVE Description)Mandiant Vulnerability Analysis CVE-2015-1179(CVE Description)Mandiant Vulnerability Analysis CVE-2023-23296(CVE Description)Mandiant Vulnerability Analysis CVE-2023-29411(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1749(CVE Description)Mandiant Vulnerability Analysis CVE-2022-30065(CVE Description)Mandiant Vulnerability Analysis CVE-2023-27464(CVE Description)Mandiant Vulnerability Analysis CVE-2023-28766(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22350(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22354(CVE Description)Mandiant Vulnerability Analysis CVE-2023-2131(CVE Description)Mandiant Vulnerability Analysis CVE-2022-32208(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1285(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22353(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22295(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22347(CVE Description)Mandiant Vulnerability Analysis CVE-2022-32205(CVE Description)Mandiant Vulnerability Analysis CVE-2022-43768(CVE Description)Mandiant Vulnerability Analysis CVE-2022-40674(CVE Description)Mandiant Vulnerability Analysis CVE-2023-28384(CVE Description)Mandiant Vulnerability Analysis CVE-2023-29169(CVE Description)Mandiant Vulnerability Analysis CVE-2022-32207(CVE Description)Mandiant Vulnerability Analysis CVE-2023-29413(CVE Description)Mandiant Vulnerability Analysis CVE-2022-1729(CVE Description)Mandiant Vulnerability Analysis CVE-2023-23294(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22419(CVE Description)Mandiant Vulnerability Analysis CVE-2022-3686(CVE Description)Mandiant Vulnerability Analysis CVE-2023-28400(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22345(CVE Description)Mandiant Vulnerability Analysis CVE-2022-43767(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22424(CVE Description)Mandiant Vulnerability Analysis CVE-2023-28716(CVE Description)Mandiant Vulnerability Analysis CVE-2021-46828(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22346(CVE Description)Mandiant Vulnerability Analysis CVE-2020-28895(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22321(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1751(CVE Description)Mandiant Vulnerability Analysis CVE-2022-32206(CVE Description)Mandiant Vulnerability Analysis CVE-2023-1750(CVE Description)Mandiant Vulnerability Analysis CVE-2023-28828(CVE Description)Mandiant Vulnerability Analysis CVE-2022-3685(CVE Description)Mandiant Vulnerability Analysis CVE-2022-3683(CVE Description)Mandiant Vulnerability Analysis CVE-2023-29412(CVE Description)Mandiant Vulnerability Analysis CVE-2023-22421(CVE Description)Mandiant Vulnerability Analysis