ICS-Oriented Intrusion and Attack Tools: Exploit Modules Released In 2022

Critical Infrastructure (CI) | Fusion (FS)

January 30, 2023 09:57:54 PM, 23-00001956, Version: 1

Executive Summary

- Exploit modules continue to be one of the most numerous cyber operation tool types given their overall simplicity and accessibility, with module creators releasing new industrial control system (ICS)-oriented modules monthly.
- Throughout 2022, Mandiant identified 62 exploits incorporated into ICS-focused exploit frameworks, 39 of which we tied to publicly known vulnerabilities or proof-of-concept code.
- ICS asset owners should monitor exploit tool creation as a risk factor and prioritize patching affected systems.

Threat Detail

Exploit modules continue to be one of the most numerous cyber operation tool types given their overall simplicity and accessibility, with module creators and framework operators releasing new industrial control system (ICS)-oriented modules monthly. Mandiant tracked modules released in 2022 targeting industrial control system (ICS)-specific vulnerabilities for the following frameworks: Metasploit, Core Impact, and Immunity Canvas. For more information on exploit modules targeting ICS assets, see ICS-Oriented Intrusion and Attack Tools: Exploit Modules for ICS Vulnerabilities.

Exploit Modules by Framework

Throughout 2022, Mandiant identified 78 ICS-specific exploit modules that collectively contain 62 exploits, as some of the exploit modules appear to likely leverage the same underlying exploit code across the three frameworks. We tied 39 of these exploits to publicly known vulnerabilities or proof-of-concept code and were unable to find additional information for the remaining 23. It is possible that some of these 23 exploits for which we could not identify a related publicly disclosed vulnerability or proof-of-concept code are zero-days.

Exploit Framework	New ICS Exploit Modules
Metasploit	19
Core Impact	32
Immunity Canvas	27

Table 1: Number of ICS exploit modules released in 2022 by framework

Exploit Modules by Vendors

In 2022, we identified exploit modules released for a total of 48 different vendors, most of which had only one or two modules released targeting their products. Figure 1 shows the top five vendors with the highest number of exploit modules released, the top two being Contec and Siemens with five modules each. We emphasize that this does not indicate which vendors are the most targeted, but which products have received the most attention from module creators and framework administrators during 2022.

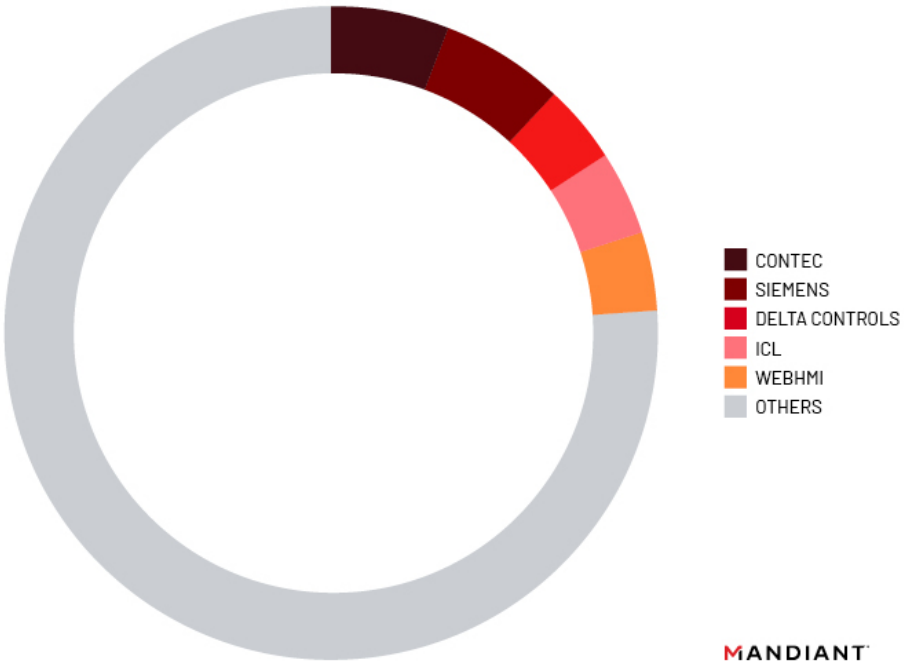

Figure 1: Top 5 vendors with the most exploit modules

- Contec is an electronic device manufacturer that produces a variety of industrial devices, with their headquarters in Japan.
    - While Contec matches Siemens for the highest number of exploit modules released in 2022, it does not indicate that Contec is frequently targeted by module creators. Prior to 2022, we have not identified any exploit modules targeting Contec products, indicating that the high number of modules this year is likely due to the public disclosure of Contec SolarView Compact vulnerabilities.
- Siemens products continue to be a high-value target for exploit modules. This is likely due to the company's global presence and the high availability of the devices.

Vulnerabilities Targeted by Exploit Modules

Of the 39 publicly known vulnerabilities, 22 of them were publicly disclosed in 2022. This indicates that module creators are active in the ICS vulnerability space, either developing modules for newly discovered vulnerabilities or identifying and incorporating public exploits into their frameworks. The disclosure year of the other 17 vulnerabilities ranges from 2006 to 2021. It should be noted that modules released for older vulnerabilities are not necessarily novel exploits, but their inclusion in popular frameworks increases the risk of exploitation as various threat actors can leverage these tools.

Vulnerabilities Exploited	Year Disclosed
CVE-2022-0983	2022
CVE-2022-2253	2022
CVE-2022-2254	2022
CVE-2022-22965	2022
CVE-2022-23854	2022
CVE-2022-24706	2022
CVE-2022-25359	2022
CVE-2022-26833	2022
CVE-2022-27480	2022
CVE-2022-29298	2022
CVE-2022-29299	2022
CVE-2022-29301	2022
CVE-2022-29303	2022

CVE-2022-29732	2022
CVE-2022-29733	2022
CVE-2022-29735	2022
CVE-2022-34753	2022
CVE-2022-35513	2022
EDB-ID: 50613	2022
EDB-ID: 50745	2022
EDB-ID: 50872	2022
EDB-ID: 50949	2022
CVE-2021-21964	2021
CVE-2021-42171	2021
CVE-2021-42750	2021
CVE-2021-42751	2021
CVE-2021-46417	2021
CVE-2020-12504	2020
CVE-2019-9193	2019
CVE-2018-10594	2018
CVE-2018-16060	2018
ZSL-2018-5495	2018
CVE-2017-20084	2017
CVE-2017-9947	2017
CVE-2015-2177	2015
CVE-2014-0780	2014
CVE-2014-0781	2014
EDB-ID: 19456	2012
CVE-2006-6488	2006

Table 2: Vulnerabilities exploited by modules sorted by year publicly disclosed

Conclusion and Mitigations

ICS intrusion and attack tools facilitate targeting sophisticated systems for a variety of threat actors. While impacting ICS can often require a high level of experience, knowledge, and intent, our threat observations show that threat actors are beginning to adopt these tools and leverage them in opportunistic attacks against ICS (22-00014563). ICS asset owners should monitor exploit tool creation as a risk factor and prioritize patching affected systems. ICS security teams can identify vulnerable systems through vulnerability scans or analysis of software/hardware versioning from either asset inventories or manual analysis of devices.

Appendix: Exploits Sorted by Vendor

Vendor	Product	Exploit Title / Type	Vulnerability	Framework
Ansys	Ansys SCADA Suite	Ansys Scade Suite Version Student 2022 R1 Remote Denial of Service	Unknown	Immunity Canvas
Ansys	Ansys SCADA Suite	famous critical embedded Ansys Scade soft. Remote DoS	Unknown	Immunity Canvas
Apache	CounchDB	CouchDB CVE-2022-24706 Remote Code Execution	CVE-2022-24706	Core Impact
AVEVA	InTouch HMI	AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal	CVE-2022-23854	Metasploit
Brainchild	Electronic Panel Studio	Brainchild Electronic Panel Studio Generated Projects Network DoS	Unknown	Immunity Canvas
Bruel and Kjaer Vibro	Compact Setup	Bruel and Kjaer Vibro Compact Setup Remote	Unknown	Immunity

	Software	DoS		Canvas
Contec	SolarView Compact	SolarView Compact Directory Traversal Vulnerability. CVE-2022-29298	CVE-2022-29298	Core Impact Immunity Canvas
Contec	SolarView Compact	SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)	CVE-2022-29299	Metasploit
Contec	SolarView Compact	SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)	CVE-2022-29301	Metasploit
Contec	SolarView Compact	SolarView Compact 6.0 - OS Command Injection	CVE-2022-29303	Metasploit
Delta Controls	enteliTOUCH	Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Scripting (XSS)	CVE-2022-29732	Metasploit
Delta Controls	enteliTOUCH	Delta Controls enteliTOUCH 3.40.3935 - Cookie User Password Disclosure	CVE-2022-29733	Metasploit
Delta Controls	enteliTOUCH	Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Request Forgery (CSRF)	CVE-2022-29735	Metasploit
Delta Electronics	COMMGR	Delta Industrial Automation COMMGR (ModBus) 1.08 Denial of Service [1Day]	CVE-2018-10594	Immunity Canvas
Eaton	Lean Automation	Eaton Lean Automation XP12inDemoProgram Directory Traversal and file disclosure. [1Day]	Unknown	Immunity Canvas
Eaton	Visual Designer	Eaton Visual Designer v7.1 software Remote Code Execution Vulnerability	Unknown	Immunity Canvas
Emerson	PAC Machine Edition	Emerson PAC Machine Edition 9.80 Build 8695 - 'TrapiServer' Unquoted Service Path	EDB-ID: 50745	Metasploit
enscada	Indigo Scada	Indigo Scada Info Disclosure.	Unknown	Core Impact
FLIR	Brickstream	FLIR Systems FLIR Brickstream 3D+ Unauthenticated Config Download.	ZSL-2018-5495	Core Impact
Franklin Fueling Systems	Colibri Controller	Franklin Fueling Systems Colibri Controller Local File Inclusion. CVE-2021-46417	CVE-2021-46417	Core Impact Immunity Canvas Metasploit
GEOVAP	Reliance SCADA	GEOVAP Reliance SCADA LicenseService Remote DoS	Unknown	Core Impact
Honeywell	PowerNet Twin Client	Honeywell PowerNet Twin Client < 8.9 (RFSync 1[.]0[.]0[.]1) Remote Denial of Service	EDB-ID: 19456	Core Impact
ICL	ScadaFlex II SCADA Controller SC-1 and SC-2	ICL ScadaFlex II SCADA Controller SC-1 and SC-2	CVE-2022-25359	Core Impact Immunity Canvas Metasploit
ICONICS	Dialog Wrapper Module	ICONICS Dialog Wrapper Module ActiveX control vulnerable to buffer overflow	CVE-2006-6488	Core Impact
ICONICS	Genesis HMI SCADA	ICONICS Genesis HMI SCADA Denial of Service. [old-0day]	Unknown	Core Impact
ICP DAS	NAPOPC_ST DA Server	ICPDAS NAPOPC_ST DA Server DOS	Unknown	Core Impact Immunity Canvas
IDAutomation	Unknown	IDAutomation bug	Unknown	Core Impact
Inductive Automation	Ignition	Inductive Automation Ignition 8.0.7 Arbitrary File Upload	Unknown	Core Impact
InduSoft	WebStudio	InduSoft WebStudio Directory Traversal and file disclosure Exploit	CVE-2014-0780	Core Impact
JUNG	Smart Panel	JUNG Smart Panel Designer Directory Traversal	Unknown	Immunity Canvas

JUNG	Smart Visu Server	JUNG Smart Visu Server Path traversal. public	CVE-2017-20084	Immunity Canvas
KeysightTechnologies	Keysight Communications Fabric	Keysight Communications Fabric Denial of Service	Unknown	Immunity Canvas
LEADTOOLS	LEADTOOLS	LEADTOOLS ltmmCapture 17.5 Arbitrary File Overwrite Vulnerability	Unknown	Immunity Canvas
Mitsubishi Electric Europe B.V.	SmartRTU	Mitsubishi Electric & INEA SmartRTU Source Code Disclose	CVE-2018-16060	Immunity Canvas
Moodle	Moodle	Moodle CVE-2022-0983 Auth SQL Injection	CVE-2022-0983	Core Impact
Open Automation Software	OAS Platform	open_automation_software_cve_2022_26833[.]py - Open Automation Software CVE-2022-26833	CVE-2022-26833	Core Impact Immunity Canvas
Pepperl+Fuchs	Comtrol RocketLinx	Comtrol RocketLinx Arbitrary File Read	CVE-2020-12504	Core Impact Immunity Canvas
PostgreSQL	PostgreSQL	PostgreSQL CVE-2019-9193 Remote Code Execution	CVE-2019-9193	Core Impact Metasploit
Powercom	UPSMON PRO	POWERCOM_UPSMON_DirTrav[.]py - POWERCOM UPSMON PRO for Windows Directory Traversal 0day	Unknown	Core Impact
Schneider Electric	SpaceLogic C-Bus	Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) - Remote Code Execution	CVE-2022-34753	Metasploit
Schneider Electric	SpaceLogic C-Bus	Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - Remote Code Execution (RCE)	EDB-ID: 50949	Metasploit
ScriptCase	ScriptCase	Scriptcase 9.7 - Remote Code Execution (RCE)	EDB-ID: 50872	Metasploit
ScriptCase	ScriptCase	ScriptCase 9.7.016 - Arbitrary File Deletion. 0day	Unknown	Core Impact
Sealevel Systems, Inc.	SeaConnect 370W	Sealevel Systems Inc. SeaConnect 370W Remote Denial of Service CVE-2021-21964	CVE-2021-21964	Immunity Canvas
Siemens	A8000	Siemens A8000 Missing Authentication Credential Disclosure. public	CVE-2022-27480	Core Impact Immunity Canvas
Siemens	BACnet	Siemens BACnet Field Panel Path Traversal	CVE-2017-9947	Core Impact
Siemens	S7-300, S7-400 PLCs	Siemens S7 Layer 2 - Denial of Service (DoS)	EDB-ID: 50613	Metasploit
Siemens	SIMATIC S7-300	Siemens SIMATIC S7-300 CPU Remote DoS	CVE-2015-2177	Core Impact
Simple-SCADA	Simple-SCADA	SIMPLE SCADA 2 DirTrav	Unknown	Core Impact Immunity Canvas
Standa	SMCVieW	Standa SMCVieW RCE Vulnerability	Unknown	Core Impact Immunity Canvas
ThingM	Blink1Control2	Blink1Control2 CVE-2022-35513 Password Decryption	CVE-2022-35513	Core Impact
ThingsBoard	ThingsBoard	ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)	CVE-2021-42750	Metasploit
ThingsBoard	ThingsBoard	ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)	CVE-2021-42751	Metasploit
Tribal Systems	Zenario	Zenario CVE-2021-42171 Auth Arbitrary File	CVE-2021-	Core Impact

		Upload	42171	
VBASE	VBASE Editor	VBASE Editor HMI SCADA DoS	Unknown	Immunity Canvas
VMWare	Spring Framework	Spring MVC or Spring WebFlux application running on JDK 9+ RCE. public	CVE-2022-22965	Core Impact
WebHMI	WebHMI	WebHMI 4[.]1[.]1[.]7662 Remote Code Execution. public	CVE-2022-2253	Immunity Canvas Metasploit
WebHMI	WebHMI	WebHMI 4.1 - Stored Cross Site Scripting (XSS) (Authenticated)	CVE-2022-2254	Metasploit
Weeder Technologies	ModCom HMI SCADA Software	ModCom HMI SCADA Software RCE via ActiveX	Unknown	Core Impact Immunity Canvas
WinSystems	C-more Simulator	WinSystems C-more v6.72 Simulator Remote Crash	Unknown	Core Impact
XISOM	X-Scada Viewer	XISOM X-Scada Viewer Directory Traversal	Unknown	Core Impact Immunity Canvas
Yokogawa	Centum CS3000	Yokogawa Centum CS3000 R3.08.50 Denial of Service. public	CVE-2014-0781	Core Impact Immunity Canvas

Table 3: List of exploits incorporated into ICS-focused exploit modules in 2022

Please rate this product by taking a short four question survey

First Version Publish Date

January 30, 2023 09:57:54 PM

Threat Intelligence Tags

Affected Industries

- Aerospace & Defense
- Agriculture
- Construction & Engineering
- Energy & Utilities
- Manufacturing
- Oil & Gas
- Pharmaceuticals
- Telecommunications
- Transportation

Affected Systems

- Control Systems and Applications
- Equipment Under Control
- Operations Management
- Regulatory and Supervisory Control
- Communication Infrastructure

Intended Effects

- Degradation
- Disruption

Tactics, Techniques And Procedures (TTPs)

- Exploit Development

Version Information

Version:1, January 30, 2023 09:57:54 PM

Common Vulnerabilities and Exposures

CVE ID:

CVE-2022-0983(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2253(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2254(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-22965(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23854(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-24706(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-25359(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-26833(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-27480(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29298(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29299(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29301(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29303(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29732(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29733(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-29735(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-34753(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-35513(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-21964(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42171(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42750(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42751(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-46417(CVE Description)Mandiant Vulnerability Analysis
CVE-2020-12504(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-9193(CVE Description)Mandiant Vulnerability Analysis
CVE-2018-10594(CVE Description)Mandiant Vulnerability Analysis
CVE-2018-16060(CVE Description)Mandiant Vulnerability Analysis
CVE-2017-9947(CVE Description)Mandiant Vulnerability Analysis
CVE-2017-20084(CVE Description)Mandiant Vulnerability Analysis
CVE-2015-2177(CVE Description)Mandiant Vulnerability Analysis
CVE-2014-0780(CVE Description)Mandiant Vulnerability Analysis
CVE-2014-0781(CVE Description)Mandiant Vulnerability Analysis
CVE-2006-6488(CVE Description)Mandiant Vulnerability Analysis

MANDIANT ADVANTAGE