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

Critical Infrastructure (CI) | Fusion (FS)

Vulnerability (VU)

April 3, 2023 12:40:03 PM, 23-00005666, 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 March 2023, CISA published 34 advisories related to vulnerabilities in ICS or medical devices.
- The advisories presented information on 166 Common Vulnerability Enumeration (CVE) IDs from which 20 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 March 2023.

ICS and Medical Vulnerability Disclosure

Mandiant Threat Intelligence extracted all Common Vulnerability Enumeration (CVE) IDs when available from advisories and identified 166 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-416: USE AFTER FREE
  - Once opened, a maliciously crafted FBX file could leverage a use-after-free vulnerability in versions of Autodesk FBX SDK prior to version 2020. Exploitation of this vulnerability could cause the application to reference a memory location controlled by an unauthorized third party and run arbitrary code on the system.
- CWE-20: IMPROPER INPUT VALIDATION
  - A type confusion vulnerability could allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial-of-service condition.

- CWE-362: CONCURRENT EXECUTION USING SHARED RESOURCE WITH IMPROPER SYNCHRONIZATION ('RACE CONDITION')
    - A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges. The bug allows to build several exploit primitives such as kernel address information leak, arbitrary execution, etc.
- CWE-611: IMPROPER RESTRICTION OF XML EXTERNAL ENTITY REFERENCE
    - Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
- CWE-367: TIME-OF-CHECK TIME-OF-USE (TOCTOU) RACE CONDITION
    - DMA attacks on the PnpSmm shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges.

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

- Baicells Nova | CISA
    -
- Akuvox E11 | CISA
    -
- AVEVA Plant SCADA and AVEVA Telemetry Server | CISA
    -
- Omron CJ1M PLC | CISA
    -
- Honeywell OneWireless Wireless Device Manager | CISA
    -
- Siemens Mendix SAML Module | CISA
    -
- Siemens SCALANCE, RUGGEDCOM Third-Party | CISA
    -
- Rockwell Automation ThinManager | CISA
    -
- Delta Electronics InfraSuite Device Master | CISA
    -
- ProPump and Controls Osprey Pump Controller | 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	3	53	31	4
Delta Electronics		1	9	3
Akuvox		3	6	4
ProPump and Controls, Inc.			5	4
Siemens ProductCERT			8	
Schneider Electric		3	5	
VISAM		7		
SAUTER		1	4	
Rockwell Automation		1	2	1
Autodesk			3	
Honeywell		1	1	1
ABB		2	1	
Baicells				1
Hitachi Energy		2		
AVEVA				1
Omron				1
Mitsubishi Electric			1	
GE Digital			1	
Keysight Technologies			1	
CP Plus			1	
RoboDK			1	
Rittal		1		
Medtronic		1		
B&R Industrial Automation		1		
Step Tools, Inc	1			

Figure 1: CVE count by vendor

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

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

Advisory	Vendor	Equipment	CVE(s)
Mitsubishi Electric MELSEC iQ-F Series | CISA	Mitsubishi Electric	MELSEC iQ-F Series	CVE-2023-0457
Baicells Nova | CISA	Baicells	Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430	CVE-2023-0776
Rittal CMC III Access	Rittal	CMC III	CVE-2022-40633

systems | CISA			
Medtronic Micro Clinician and InterStim Apps | CISA	Medtronic	Micros Clinician (A51200) app and InterStim X Clinician (A51300) app	CVE-2023-25931
Hitachi Energy Relion 670, 650 and SAM600-IO Series | CISA	Hitachi Energy	Relion 670, 650, and SAM600-IO Series	CVE-2022-3864
Step Tools Third-Party | CISA	Step Tools, Inc	STEPTools ifcmesh library	CVE-2023-0973
B&R Systems Diagnostics Manager | CISA	B&R Industrial Automation	Systems Diagnostics Manager (SDM)	CVE-2022-4286
ABB Ability Symphony Plus | CISA	ABB	Ability Symphony Plus	CVE-2023-0228
Akuvox E11 | CISA	Akuvox	E11	CVE-2023-0343, CVE-2023-0355, CVE-2023-0354, CVE-2023-0353, CVE-2023-0352, CVE-2023-0351, CVE-2023-0350, CVE-2023-0349, CVE-2023-0348, CVE-2023-0347, CVE-2023-0346, CVE-2023-0345, CVE-2023-0344
AVEVA Plant SCADA and AVEVA Telemetry Server | CISA	AVEVA	AVEVA Plant SCADA and AVEVA Telemetry Server	CVE-2023-1256
GE iFIX | CISA	GE Digital	iFIX	CVE-2023-0598
Autodesk FBX SDK | CISA	Autodesk	FBX SDK	CVE-2022-41302, CVE-2022-41303, CVE-2022-41304
Omron CJ1M PLC | CISA	Omron	CJ1M PLC	CVE-2023-0811
Rockwell Automation Modbus TCP	Rockwell Automation	Modbus TCP Server Add-On	CVE-2023-0027

AOI Server | CISA		Instruction (AOI)	
Honeywell OneWireless Wireless Device Manager | CISA	Honeywell	OneWireless Wireless Device Manager (WDM)	CVE-2022-46361, CVE-2022-43485, CVE-2022-4240
Siemens Mendix SAML Module | CISA	Siemens	Mendix SAML Module	CVE-2023-25957
Siemens SCALANCE W1750D Devices | CISA	Siemens	SCALANCE W1750D	CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286
Siemens RUGGEDCOM CROSSBOW V5.2 | CISA	Siemens	RUGGEDCOM CROSSBOW	CVE-2023-27309, CVE-2023-27310
Siemens RUGGEDCOM CROSSBOW V5.3 | CISA	Siemens	RUGGEDCOM CROSSBOW	CVE-2023-27462, CVE-2023-27463
Siemens SCALANCE, RUGGEDCOM Third-Party | CISA	Siemens	Busybox Applet affecting SCALANCE and RUGGEDCOM products	CVE-2018-25032, CVE-2019-1073, CVE-2019-1071, CVE-2019-1125, CVE-2021-4034, CVE-2021-4149, CVE-2017-5715, CVE-2021-26401, CVE-2021-42373, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386, CVE-2022-0001, CVE-2022-0002, CVE-2022-0494, CVE-2022-0547, CVE-2022-1011, CVE-2022-1016, CVE-2022-1198, CVE-2022-1199, CVE-2022-1292, CVE-2022-1304, CVE-2022-1343, CVE-2022-1353, CVE-2022-1473, CVE-2022-1516, CVE-2022-1652, CVE-2022-1729, CVE-2022-1734, CVE-2022-1974, CVE-2022-1975, CVE-2022-2380, CVE-2022-2588, CVE-2022-2639, CVE-2022-20158, CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-

			CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042, CVE-2022-23308, CVE-2022-26490, CVE-2022-28356, CVE-2022-28390, CVE-2022-30065, CVE-2022-30594, CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-32296, CVE-2022-32981, CVE-2022-33981, CVE-2022-35252, CVE-2022-36879, CVE-2022-36946
Siemens SCALANCE Third-Party | CISA	Siemens	Various third-party components used in SCALANCE W-700 devices	CVE-2018-12886, CVE-2018-25032, CVE-2021-42373, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386, CVE-2022-23395
Rockwell Automation ThinManager | CISA	Rockwell Automation	ThinManager ThinServer	CVE-2023-27855, CVE-2023-27856, CVE-2023-27857
VISAM VBASE Automation Base | CISA	VISAM	VBASE	CVE-2022-41696, CVE-2022-43512, CVE-2022-45121, CVE-2022-45468, CVE-2022-45876, CVE-2022-46286, CVE-2022-46300
Siemens RADIUS Client of SIPROTEC 5 Devices | CISA	Siemens ProductCERT	RADIUS client of SIPROTEC 5 devices	CVE-2022-38767
Siemens RUGGEDCOM APE1808 Product Family | CISA	Siemens ProductCERT	RUGGEDCOM APE1808 Product Family	CVE-2022-32469, CVE-2022-32470, CVE-2022-32471, CVE-2022-32475, CVE-2022-32477, CVE-2022-32953, CVE-2022-32954
Delta Electronics InfraSuite Device Master | CISA	Delta Electronics	InfraSuite Device Master	CVE-2023-1133, CVE-2023-1139, CVE-2023-1145, CVE-2023-1138, CVE-2023-1144, CVE-2023-1137, CVE-2023-1143, CVE-2023-1134, CVE-2023-1142, CVE-2023-1136, CVE-2023-1141, CVE-2023-1135, CVE-2023-1140
Keysight N6845A Geolocation Server | CISA	Keysight Technologies	N6854A Geolocation Sever	CVE-2023-1399
ProPump and	ProPump	Osprey Pump	CVE-2023-28395, CVE-2023-28375, CVE-2023-28654, CVE-

Controls Osprey Pump Controller | CISA	and Controls, Inc.	Controller	2023-27886, CVE-2023-27394, CVE-2023-28648, CVE-2023-28398, CVE-2023-28718, CVE-2023-28712
ABB Pulsar Plus Controller | CISA	ABB	Pulsar Plus Controller	CVE-2022-1607, CVE-2022-26080
Schneider Electric IGSS | CISA	Schneider Electric	IGSS (Interactive Graphical SCADA System)	CVE-2023-27980, CVE-2023-27982, CVE-2023-27978, CVE-2023-27981, CVE-2023-27984, CVE-2023-27977, CVE-2023-27979, CVE-2023-27983
SAUTER EY-modulo 5 Building Automation Stations | CISA	SAUTER	EY-modulo 5 Building Automation Stations	CVE-2023-28650, CVE-2023-28655, CVE-2023-22300, CVE-2023-27927, CVE-2023-28652
CP Plus KVMS Pro | CISA	CP Plus	KVMS Pro	CVE-2023-1518
RoboDK | CISA	RoboDK	RoboDK	CVE-2023-1516
Hitachi Energy IEC 61850 MMS-Server | CISA	Hitachi Energy	IEC 61850 MMS-Server	CVE-2022-3353

Table 1: CISA advisories for March 2023

First Version Publish Date

April 3, 2023 12:40:03 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, April 3, 2023 12:40:03 PM

Common Vulnerabilities and Exposures

CVE ID:

CVE-2023-1143(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23395(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0345(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-45121(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0343(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0351(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1516(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27855(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0457(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1734(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28650(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27982(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2639(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-46286(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1607(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32953(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28395(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42382(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1134(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-4450(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-25931(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23038(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41304(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0215(CVE Description)Mandiant Vulnerability Analysis

CVE-2019-1071(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28398(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1011(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-0001(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32205(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1142(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1139(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0228(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32477(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0776(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1137(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2588(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27856(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27463(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28648(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-33981(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1140(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-4149(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43512(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0811(CVE Description)Mandiant Vulnerability Analysis
CVE-2018-25032(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42373(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32954(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23042(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42376(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32470(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42378(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-46300(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1292(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1138(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1145(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0355(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32208(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23036(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-38767(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0027(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1399(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-0494(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0350(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32207(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27886(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27978(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32475(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0346(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3353(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-4240(CVE Description)Mandiant Vulnerability Analysis
CVE-2017-5715(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1516(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1144(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-0547(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1256(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1136(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-35252(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-46361(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-1073(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-36946(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32469(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42380(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0352(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27309(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-45876(CVE Description)Mandiant Vulnerability Analysis
CVE-2019-1125(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42381(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42377(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23308(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0349(CVE Description)Mandiant Vulnerability Analysis

CVE-2023-0354(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23041(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27927(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1473(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-4034(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27979(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23037(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42385(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-36879(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1016(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42375(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0598(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41696(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42383(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42386(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-28390(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1975(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-30065(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-43485(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-20158(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1652(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-30594(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32296(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23039(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1135(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1199(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28712(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0973(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1304(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1343(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-0002(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-26490(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27983(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0353(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1729(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41303(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-23040(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27857(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-22300(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27977(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32471(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1353(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27984(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27462(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28718(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1974(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-28356(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27310(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-1198(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27394(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-4286(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-2380(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28375(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-25957(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0347(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1133(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32981(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-4304(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0286(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42374(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-26080(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-45468(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42384(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0344(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27980(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28652(CVE Description)Mandiant Vulnerability Analysis

CVE-2023-28654(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-0348(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-3864(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1518(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-42379(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-27981(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-40633(CVE Description)Mandiant Vulnerability Analysis
CVE-2021-26401(CVE Description)Mandiant Vulnerability Analysis
CVE-2018-12886(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-32206(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-28655(CVE Description)Mandiant Vulnerability Analysis
CVE-2023-1141(CVE Description)Mandiant Vulnerability Analysis
CVE-2022-41302(CVE Description)Mandiant Vulnerability Analysis

MANDIANT ADVANTAGE

german[.]simkin@mandiant.com