

Search the blog

[Research Threat intelligence Microsoft Defender for IoT Vulnerabilities and exploits](#)

10 min read

## Multiple high severity vulnerabilities in CODESYS V3 SDK could lead to RCE or DoS

By [Microsoft Threat Intelligence](#)

August 10, 2023



IoT security

Microsoft Defender

Microsoft Defender Threat Intelligence

IoT / OT threats

Remote code execution

Microsoft's cyberphysical system researchers recently identified multiple high-severity vulnerabilities in the CODESYS V3 software development kit (SDK), a software development environment widely used to program and engineer programmable logic controllers (PLCs). Exploitation of the discovered vulnerabilities, which affect all versions of CODESYS V3 prior to version 3.5.19.0, could put operational technology (OT) infrastructure at risk of attacks, such as remote code execution (RCE) and denial of service (DoS). The discovery of these vulnerabilities highlights the critical importance of ensuring the security of industrial control systems and underscores the need for continuous monitoring and protection of these environments.

CODESYS is [compatible](#) with approximately 1,000 different device types from over 500 manufacturers and several million devices that use the solution to implement the international industrial standard IEC (International Electrotechnical Commission) 61131-3. A DoS attack against a device using a vulnerable version of CODESYS could enable threat actors to shut down a power plant, while remote code execution could create a backdoor for devices and let attackers tamper with operations, cause a PLC to run in an unusual way, or steal critical information. Exploiting the discovered vulnerabilities, however, requires user authentication, as well as deep knowledge of the proprietary protocol of CODESYS V3 and the structure of the different services that the protocol uses.

Microsoft researchers reported the discovery to CODESYS in September 2022 and worked closely with CODESYS to ensure that the vulnerabilities are patched. Information on the patch released by CODESYS to address these vulnerabilities can be found here: [Security update for CODESYS Control V3](#). We strongly urge CODESYS users to apply these [security updates](#) as soon as possible. We also thank CODESYS for their collaboration and recognizing the urgency in addressing these vulnerabilities.

Below is a list of the discovered vulnerabilities discussed in this blog:

CVE	CODESYS component	CVSS score	Impact
<a href="#">CVE-2022-47379</a>	CMPPapp	8.8	DoS, RCE
<a href="#">CVE-2022-47380</a>	CMPPapp	8.8	
<a href="#">CVE-2022-47381</a>	CMPPapp	8.8	
<a href="#">CVE-2022-47382</a>	CmpTraceMgr	8.8	
<a href="#">CVE-2022-47383</a>	CmpTraceMgr	8.8	
<a href="#">CVE-2022-47384</a>	CmpTraceMgr	8.8	
<a href="#">CVE-2022-47385</a>	CmpAppForce	8.8	
<a href="#">CVE-2022-47386</a>	CmpTraceMgr	8.8	
<a href="#">CVE-2022-47387</a>	CmpTraceMgr	8.8	
<a href="#">CVE-2022-47388</a>	CmpTraceMgr	8.8	
<a href="#">CVE-2022-47389</a>	CMPTTraceMgr	8.8	DoS
<a href="#">CVE-2022-47390</a>	CMPTTraceMgr	8.8	
<a href="#">CVE-2022-47391</a>	CMPDevice	7.5	
<a href="#">CVE-2022-47392</a>	CmpApp/ CmpAppBP/ CmpAppForce	8.8	
<a href="#">CVE-2022-47393</a>	CmpFiletransfer	8.8	

In this blog, we provide an overview of the CODESYS V3 protocol structure, highlighting several key components, and describe the main issue that led to our discovery of the vulnerabilities. The full research and the results can be found in our report on [Github](#). We also provide an [open-source forensics tool](#) to help users identify impacted devices, security recommendations for those affected, and detection information for potentially related threats.

## CODESYS: A widely used PLC solution

CODESYS is a software development environment that provides automation specialists with tools for developing automated solutions. CODESYS is a platform-independent solution that helps device manufacturers implement the international industrial standard IEC 61131-3. The SDK also has management software that runs on Windows machines and a simulator for testing environments, allowing users to test their PLC systems before deployment. The proprietary protocols used by CODESYS use either UDP or TCP for communication between the management software and PLC.

CODESYS is widely used and can be found in several industries, including factory automation, energy automation, and process automation, among others.



Figure 1. CODESYS devices exposed to the internet (based on Microsoft Defender Threat Intelligence data)

## Discovering the CODESYS vulnerabilities

The vulnerabilities were uncovered by Microsoft researchers while examining the security of the CODESYS V3 proprietary protocol as part of our goal to improve the security standards and create forensic tools for OT devices. During this research, we

examined the structure and security of the protocol that is used by many types and vendors of PLCs. We examined the following two PLCs that use CODESYS V3 from different vendors: Schneider Electric Modicon TM251 and WAGO PFC200.



Figure 2. The two examined PLCs

## CODESYS V3 protocol

The CODESYS network protocol works over either TCP or UDP:

- Ports 11740-11743 for TCP
- Ports 1740-1743 for UDP

The CODESYS network protocol consists of four layers:

1. **Block driver layer:** The layer that creates the capability to communicate over a physical or software interface, over TCP or UDP.
2. **Datagram layer:** The layer that enables communication between components and endpoints through physical or virtual interfaces.
3. **Channel layer:** The layer that is responsible for creating, managing, and closing communications channels.
4. **Services layer:** Represents a combination of several layers of the ISO/OSI model session layer, presentation layer, and application layer. It consists of components, each of which is responsible for a portion of functionality of the PLC and has services that it supports. Other tasks of the Services layer include encoding/decoding and encrypting/decrypting the data transmitted on that layer. Additionally, the Services layer is also responsible for tracking the client-server session. Each component is identified by a unique ID, such as:

Component name	Component ID
<i>CmpApp</i>	0x2
<i>CmpAlarmManager</i>	0x18
<i>CmpAppBP</i>	0x12
<i>CmpAppForce</i>	0x13
<i>CmpCodeMeter</i>	0x1D

These components use the Tags layer for data transmission and encoding, which is transmitted over the Services layer.

There are two types of tags: *parent* and *data*. Both tags have identical structure but different sizes and purposes. The following table provides the basic structure of tags:

Field	Parent tag size (in bytes)	Data tag size (in bytes)	Description
Tag ID	2	1	The tag ID. The value of the most significant bit determines the type of tag. For parent tag, the value of the most significant bit is set.
Tag size	2	1	The size of the data.
Tag data	(Tag size)	(Tag size)	The data of the tag.

Tags can represent any type of data, and it is extracted by the component. The difference between a parent tag and a data tag is that a parent tag is used for linking several tags into one logical element.

Tags contain several important structures, including *BTagReader* and *BTagWriter*, which include the following fields:

- Data
- Current position in data
- Size of data

These structures are allocated for each request and exist only in the context of the request. Each request handler creates *BTagWriter* and *BTagReader* tags and uses them to parse and handle requests. Tag IDs are not unique across services, meaning each service may have its own definition for a tag ID. Tag IDs are handled in the context of each service.

The following figure provides an example of a Tag layer and relevant fields.



Figure 3. Example of Tags layer fields

This example contains the following tags:

- Tag1 – )TAG ID 0x01( 10 00 00 00
- Tag2 – (TAG ID 0x23) Authentication method type
- Tag3 – (TAG ID 0x81) Parent tag that contains two sub tags
- Tag4 – (TAG ID 0x10) Username tag
- Tag5 – (TAG ID 0x11) Hash of a password tag

## CODESYS components

CODESYS consists of components and each component is responsible for a portion of functionality of the PLC. The following is a list of example components:

- [CmpAlarmManger](#) – Manages alarm events, registers clients that receive events, etc.
- [CmpApp](#) – Manages running applications and application event usage.
- [CmpAppBp](#) – Manages breakpoints in IEC tasks.
- [CmpCodeMeter](#) – Manages the CodeMeter License containers.
- [CmpCoreDump](#) – Manages creating, reading, and printing to file core dumps.
- [CMPTraceMgr](#) – Enables tracing of information inside the IEC tasks.

Each component includes a number of services that the client can ask to use. For example, *CMPTraceMgr* includes the following:

- [TraceMgrPacketCreate](#) – Creates a new trace packet
- [TraceMgrPacketDelete](#) – Deletes a trace manager packet
- [TraceMgrPacketStart](#) – Starts tracing, which is triggered by the *TraceTrigger*
- [TraceMgrRecordUpdate](#) – Records the current value of the *TraceVariable* together with the current timestamp
- [TraceMgrRecordAdd](#) – Creates a new *TraceRecordConfiguration* and adds it to a specific trace packet for a specific IEC task/application

Each service is identified by a unique number for the specific component.

## Tags layer vulnerability

A security issue was discovered inside the tag decoding mechanism that led to multiple vulnerabilities that could put devices at risk of attacks such as RCE and DoS.

In order to understand the security issue, let's analyze the service *TraceMgrRecordAdd* of the component *CMPTraceMgr* by examining the code that activates the relevant service.



Figure 4. *CMPTraceMgr*'s code that runs the wanted service

The *TraceMgrRecordAddByTag* appears to correspond to *TraceMgrRecordAdd*.

As displayed in Figure 5, the following code initializes structure from tags that are sent to the service.



Figure 5. *TraceMgrRecordAddByTag's* piece of code

The following figure looks at the code for the *TraceMgrAddNewRecordPartByTag* method, which copies data from different tags into an output buffer.



Figure 6. *TraceMgrAddNewRecordPartByTag's* piece of code

**The whole tag is copied into the buffer without validating the size, causing buffer overflow.**

Fifteen places in CODESYS V3 SDK were found with the same issue in different components that could lead to remote attackers gaining full control over the device.

## Exploitation approach

We were able to apply 12 of the buffer overflow vulnerabilities to gain RCE of PLCs. Exploiting the vulnerabilities requires user authentication as well as bypassing the Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) used by both the PLCs. To overcome the user authentication, we used a known vulnerability, [CVE-2019-9013](#), which allows us to perform a replay attack against the PLC using the unsecured username and password's hash that were sent during the sign-in process, allowing us to bypass the user authentication process.

## IEC tasks

IEC tasks are the execution unit of CODESYS runtime. It is the equivalent to thread in operating systems. A single component can have more than one task and will have at least one IEC task. The tasks are managed by CODESYS runtime.

Each IEC task has a memory segment with read, write, and execute permissions. If a threat actor writes code there, it could be run without the data execution prevention mitigation being applied.

The IEC task segment is also where the stack is defined, meaning we don't need to handle DEP.

Since the IEC tasks are part of the CODESYS code, they are present on all PLCs of all vendors that utilize CODESYS.

## Full exploit

By looking for gadgets, we can bypass the ASLR. In the examples below, we can see part of the gadgets that we used in our exploit.



Figure 7. Searching for gadgets – Schneider Electric TM251MESE

The complete exploit steps:

1. Steal credentials with CVE-2019-9013.
2. Create a new channel for the attack.
3. Sign-in to the device with the stolen credentials.
4. Exploit the vulnerabilities with a malicious packet that triggers buffer overflow.
5. Gain full control of the device.

We were able to exploit the two PLCs that we researched.

Demo video:

## Critical importance of ICS security

With CODESYS being used by many vendors, one vulnerability may affect many sectors, device types, and verticals, let alone multiple vulnerabilities. All the vulnerabilities can lead to DoS and 1 RCE. While exploiting the discovered vulnerabilities requires deep knowledge of the proprietary protocol of CODESYS V3 as well as user authentication (and additional permissions are required for an account to have control of the PLC), a successful attack has the potential to inflict great damage on targets. Threat actors could launch a DoS attack against a device using a vulnerable version of CODESYS to shut down industrial operations or exploit the RCE vulnerabilities to deploy a backdoor to steal sensitive data, tamper with operations, or force a PLC to operate in a dangerous way.

## Mitigation and protection guidance

CODESYS V3 versions prior to 3.5.19.0 are vulnerable to the discovered vulnerabilities. It is recommended to first identify the devices using CODESYS in your network and check with device manufacturers to determine which version of the CODESYS SDK is used and whether a patch is available. It is also recommended to [update the device firmware](#) to version 3.5.19.0 or above.

General recommendations:

- Apply patches to affected devices in your network. Check with the device manufacturers for available patches and [update the device firmware](#) to version 3.5.19.0 or above.
- Make sure all critical devices, such as PLCs, routers, PCs, etc., are disconnected from the internet and segmented, regardless of whether they run CODESYS.
- Limit access to CODESYS devices to authorized components only.
- Due to the nature of the CVEs, which still require a username and password, if prioritizing patching is difficult, reduce risk by ensuring proper segmentation, requiring unique usernames and passwords, and reducing users that have writing authentication.

To assist with identifying impacted devices, the cyberphysical systems research team has released an [open-source software tool](#) on GitHub that allows users to communicate with devices in their environment that run CODESYS and extract the version of CODESYS on their devices in a safe manner to confirm if their devices are vulnerable. In addition, the cyberphysical system research team also released a tool for performing a [forensics investigation](#) on CODESYS V3 devices as part of its arsenal of open-source tools available on GitHub.

## Microsoft 365 Defender detections

Microsoft 365 Defender is becoming Microsoft Defender XDR. [Learn more.](#)

### Microsoft Defender for IoT

Microsoft Defender for IoT with all versions of the sensor and TI package after April 2023 provides the following protections against these vulnerabilities and associated exploits and other malicious behavior:

- Defender for IoT detects and classifies devices that use CODESYS.
- Defender for IoT raises [alerts](#) on unauthorized access to devices using CODESYS, and abnormal behavior in these devices.
- Defender for IoT raises alerts if a threat actor attempts to exploit these vulnerabilities. Alert type: **"Suspicion of Malicious Activity"**

### Microsoft Defender Threat Intelligence

Microsoft Defender Threat Intelligence shows devices running CODESYS that are exposed to the internet by searching for

"CODESYS" components on IPs.

**Vladimir Tokarev**

*Microsoft Threat Intelligence Community*

## References

- <https://www.codesys.com/the-system/codesys-inside.html>
- <https://store.codesys.com/engineering/codesys.html>
- <https://github.com/microsoft/CoDe16/tree/main>
- <https://store.codesys.com/en/alarm-manager.html>
- <https://content.helpme-codesys.com/en/libs/CmpApp/Current/index.html>
- <https://content.helpme-codesys.com/en/libs/CmpAppBP/Current/index.html>
- <https://content.helpme-codesys.com/en/libs/CmpCodeMeter/Current/index.html>
- <https://content.helpme-codesys.com/en/libs/CmpTraceMgr/Current/index.html>
- <https://content.helpme-codesys.com/en/libs/CmpApp/Current/AppStartApplication.html>
- <https://help.codesys.com/webapp/TraceMgrPacketCreate;product=CmpTraceMgr;version=3.5.16.0>
- <https://help.codesys.com/webapp/TraceMgrPacketDelete;product=CmpTraceMgr;version=3.5.16.0>
- <https://help.codesys.com/webapp/TraceMgrPacketStart;product=CmpTraceMgr;version=3.5.16.0>
- <https://help.codesys.com/webapp/TraceMgrRecordUpdate;product=CmpTraceMgr;version=3.5.16.0>
- <https://help.codesys.com/webapp/TraceMgrRecordAdd;product=CmpTraceMgr;version=3.5.17.0>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9013>
- <https://customers.codesys.com/index.php?elD=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=>
- <https://www.codesys.com/download>
- [https://download.schneider-electric.com/files?p\\_Doc\\_Ref=SEVD-2023-192-04&p\\_enDocType=Security+and+Safety+Notice&p\\_File\\_Name=SEVD-2023-192-04.pdf&\\_ga=2.25212925.1579834642.1689503846-267712980.1687697317](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-192-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-192-04.pdf&_ga=2.25212925.1579834642.1689503846-267712980.1687697317)
- <https://cert.vde.com/de/advisories/VDE-2023-026/>
- <https://ics-cert.kaspersky.com/publications/reports/2019/09/18/security-research-codesys-runtime-a-plc-control-framework-part-1/>
- <https://ics-cert.kaspersky.com/publications/reports/2019/09/18/security-research-codesys-runtime-a-plc-control-framework-part-2/>
- <https://ics-cert.kaspersky.com/publications/reports/2019/09/18/security-research-codesys-runtime-a-plc-control-framework-part-3/>

## Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: <https://aka.ms/threatintelblog>.

To get notified about new publications and to join discussions on social media, follow us on Twitter at <https://twitter.com/MsftSecIntel>.

## Related Posts





[Research](#)

[Threat intelligence](#)

[Microsoft Defender](#)

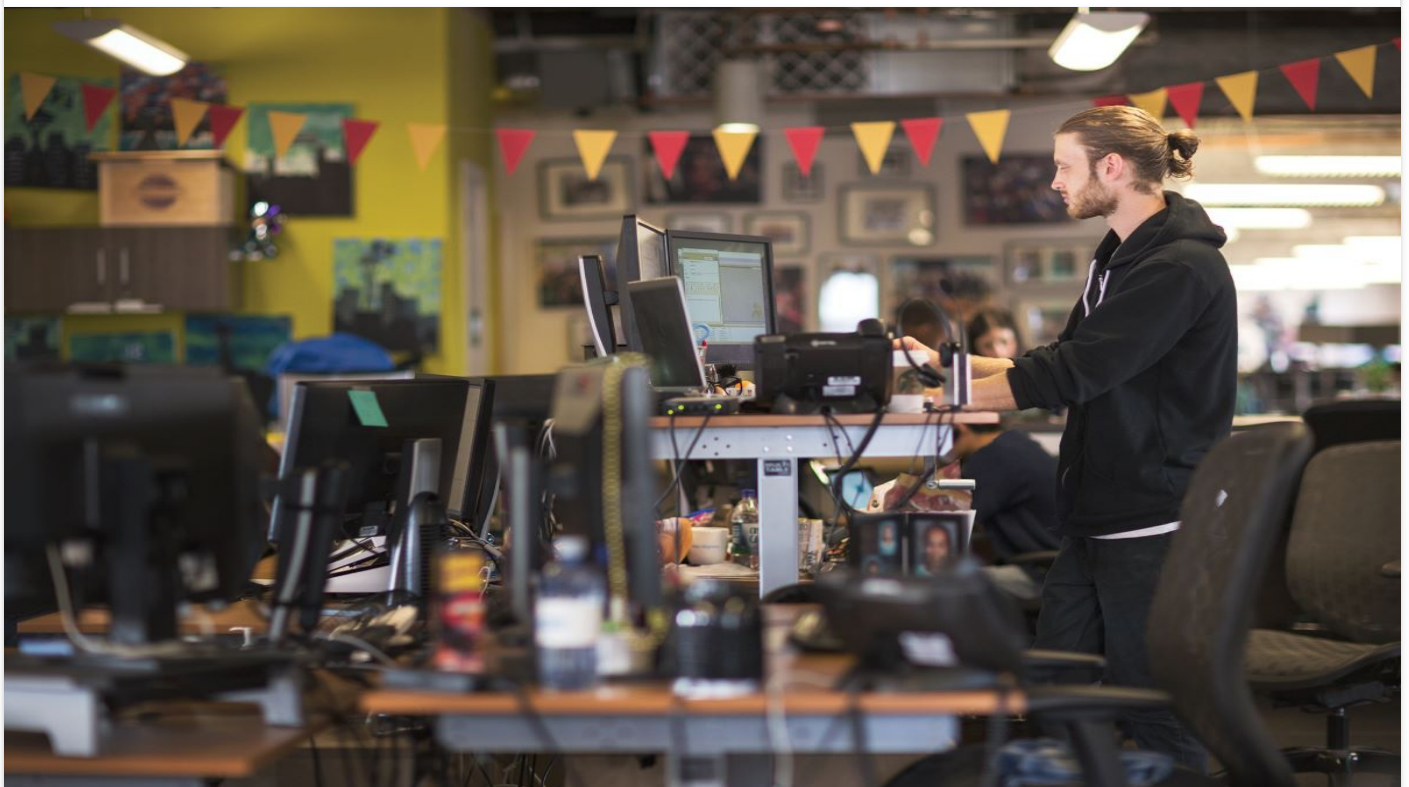
[IoT / OT threats](#)

Jun 22

11 min read

## [IoT devices and Linux-based systems targeted by OpenSSH trojan campaign](#) > >

Microsoft has uncovered an attack leveraging custom and open-source tools to target internet-facing IoT devices and Linux-based systems. The attack involves deploying a patched version of OpenSSH on affected devices to allow root login and the hijack of SSH credentials.



[Research](#)

[Threat intelligence](#)

[IoT / OT threats](#)

Dec 21

12 min read

## [Microsoft research uncovers new Zerobot capabilities](#) > >



The Microsoft Defender for IoT research team details information on the recent distribution of a Go-based botnet, known as Zerobot, that spreads primarily through IoT and web-application vulnerabilities.



[Research](#)

[Threat intelligence](#)

[Microsoft Defender](#)

[IoT / OT threats](#)

Dec 15

9 min read

## [MCCrash: Cross-platform DDoS botnet targets private Minecraft servers > >](#)

The Microsoft Defender for IoT research team analyzed a cross-platform botnet that infects both Windows and Linux systems from PCs to IoT devices, to launch distributed denial of service (DDoS) attacks against private Minecraft servers.





[Research](#)

[Threat intelligence](#)

[Microsoft Defender](#)

[Supply chain attacks](#)

Nov 22

6 min read

## Vulnerable SDK components lead to supply chain risks in IoT and OT environments > >

As vulnerabilities in network components, architecture files, and developer tools have become an increasingly popular attack vector to leverage access into secure networks and devices, Microsoft identified such a vulnerable component and found evidence of a supply chain risk that might affect millions of organizations and devices.

## Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

[Learn more](#)

Connect with us on social



### What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

### Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

[Order tracking](#)

[Certified Refurbished](#)

[Microsoft Store Promise](#)

[Flexible Payments](#)

## Education

[Microsoft in education](#)

[Devices for education](#)

[Microsoft Teams for Education](#)

[Microsoft 365 Education](#)

[How to buy for your school](#)

[Educator training and development](#)

[Deals for students and parents](#)

[Azure for students](#)

## Business

[Microsoft Cloud](#)

[Microsoft Security](#)

[Dynamics 365](#)

[Microsoft 365](#)

[Microsoft Power Platform](#)

[Microsoft Teams](#)

[Copilot for Microsoft 365](#)

[Small Business](#)

## Developer & IT

[Azure](#)

[Developer Center](#)

[Documentation](#)

[Microsoft Learn](#)

[Microsoft Tech Community](#)

[Azure Marketplace](#)

[AppSource](#)

[Visual Studio](#)

## Company

[Careers](#)

[About Microsoft](#)

[Company news](#)


[Privacy at Microsoft](#)


[Investors](#)

[Diversity and inclusion](#)

[Accessibility](#)

[Sustainability](#)

 [English \(United States\)](#)

 [Your Privacy Choices](#)

[Consumer Health Privacy](#)

[Sitemap](#) [Contact Microsoft](#) [Privacy](#) [Terms of use](#) [Trademarks](#) [Safety & eco](#) [Recycling](#) [About our ads](#) [© Microsoft 2024](#)