Kaspersky Industrial
Cybersecurity
Conference 2024

OT Vulnerability Research

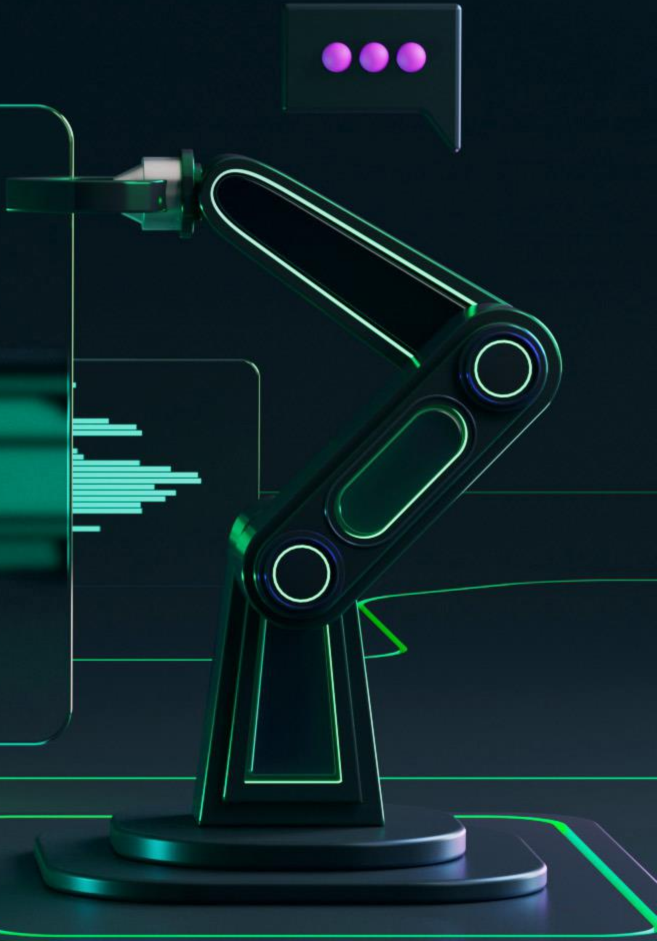
Why open source vulnerability databases are not good for ICS

kaspersky

Kaspersky Industrial Cybersecurity Conference 2024

Artem Zinenko

Head of ICS CERT Vulnerability Research and Assessment



kaspersky

Rockwell Automation

gemalto

Schneider Electric

BOSCH

SIEMENS

MITSUBISHI ELECTRIC

GE

WAGO

Telit Cinterion

MOXA®

OPC® FOUNDATION

AVEVA

Honeywell

YOKOGAWA

CODESYS

flexera

UNISOC

EMERSON™

The talk is about

- ICS Vulnerability Databases
- Data Quantity Problems
- Data Quality Problems

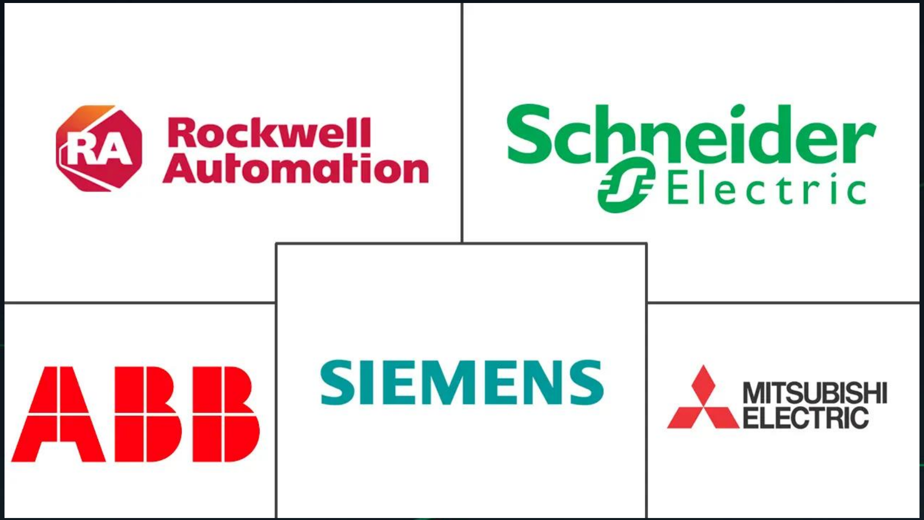
Information sources

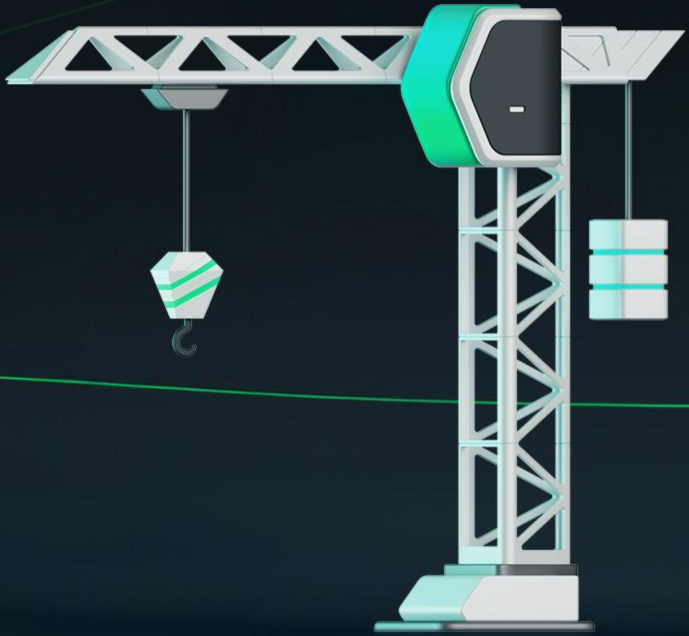
Vendor advisories

CISA (ICS/US-CERT)

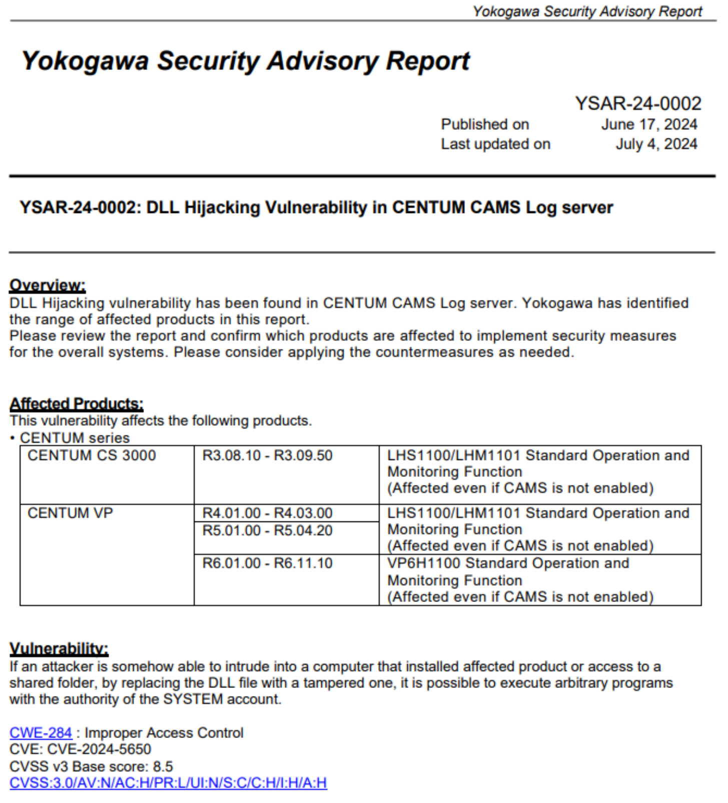
CVE Project (MITRE) / NVD

Vendor Advisories





Vendor advisories: Human-Readable Data



Yokogawa Security Advisory Report

Yokogawa Security Advisory Report

YSAR-24-0002

Published on June 17, 2024
Last updated on July 4, 2024

YSAR-24-0002: DLL Hijacking Vulnerability in CENTUM CAMS Log server

Overview:
DLL Hijacking vulnerability has been found in CENTUM CAMS Log server. Yokogawa has identified the range of affected products in this report.
Please review the report and confirm which products are affected to implement security measures for the overall systems. Please consider applying the countermeasures as needed.

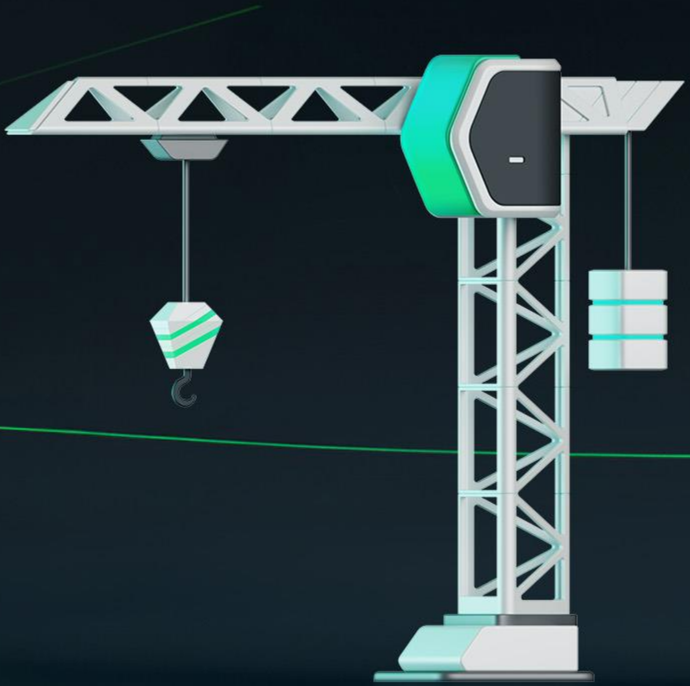
Affected Products:
This vulnerability affects the following products.

- CENTUM series

CENTUM CS 3000	R3.08.10 - R3.09.50	LHS1100/LHM1101 Standard Operation and Monitoring Function (Affected even if CAMS is not enabled)
CENTUM VP	R4.01.00 - R4.03.00 R5.01.00 - R5.04.20	LHS1100/LHM1101 Standard Operation and Monitoring Function (Affected even if CAMS is not enabled)
	R6.01.00 - R6.11.10	VP6H1100 Standard Operation and Monitoring Function (Affected even if CAMS is not enabled)

Vulnerability:
If an attacker is somehow able to intrude into a computer that installed affected product or access to a shared folder, by replacing the DLL file with a tampered one, it is possible to execute arbitrary programs with the authority of the SYSTEM account.

CWE-284 : Improper Access Control
CVE: CVE-2024-5650
CVSS v3 Base score: 8.5
CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H



https://web-material3.yokogawa.com/1/36044/files/YSAR-24-0002-E.pdf

Siemens CSAF: Machine-Readable Data

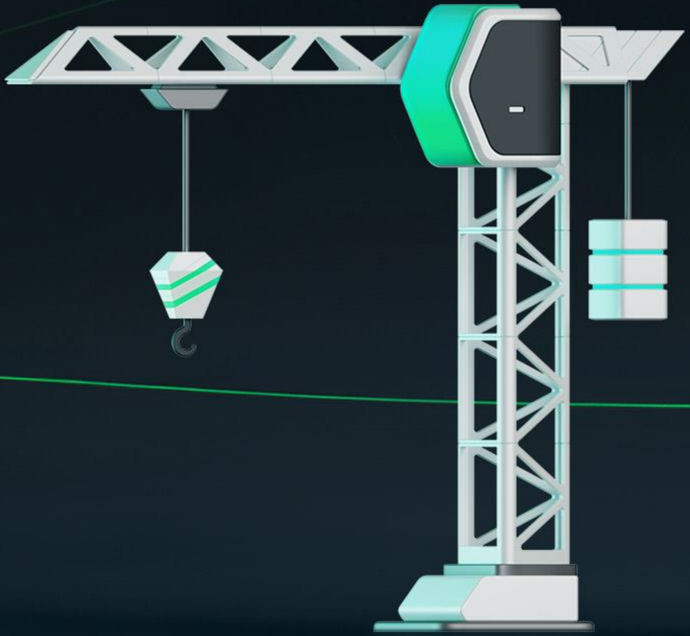
```
"vulnerabilities": [
  {
    "cve": "CVE-2024-43647",
    "cwe": {
      "id": "CWE-400",
      "name": "Uncontrolled Resource Consumption"
    },
    ...
    "product_status": {
      "known_affected": [
        ...
      ]
    },
    ...
  }
]
```

https://cert-portal.siemens.com/productcert/csaf/ssa-969738.json

Problems

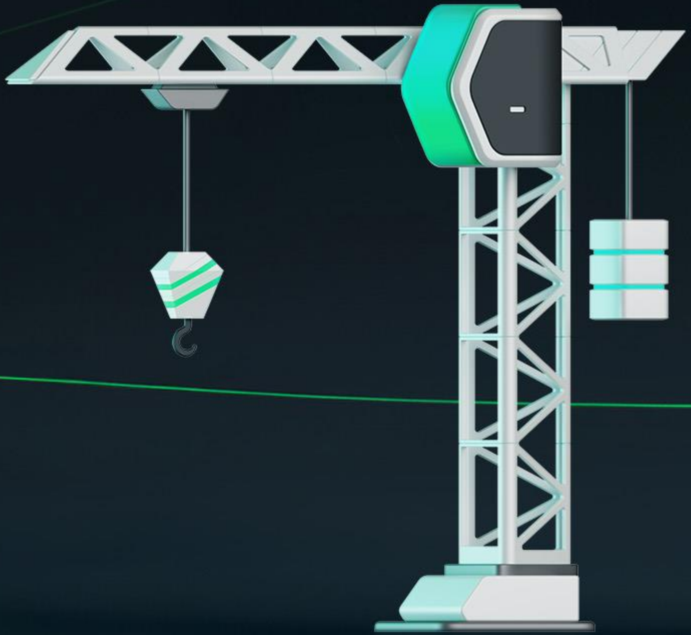
- Vulnerabilities of only one vendor
- Human-readable data (for most vendors)

CISA (ICS/US-CERT)



CISA: Missing ICS Vulnerabilities

23% ICS vulns are missing from CISA



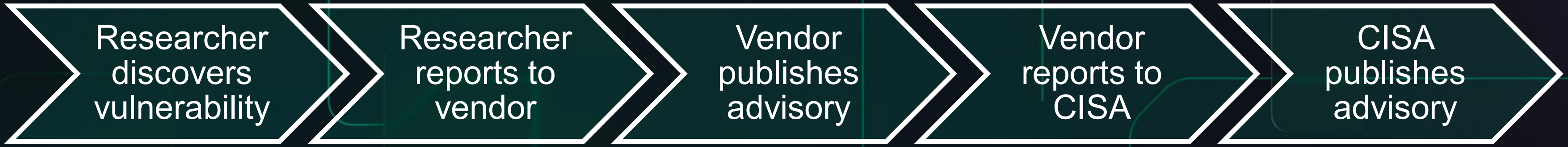
The Example of Missing Vulnerability: CVE-2018-7760

An authorization bypass vulnerability exists in Schneider Electric's Modicon M340, Modicon Premium, Modicon Quantum PLC, BMXNOR0200.

CVSSv3: **9.8**

https://nvd.nist.gov/vuln/detail/CVE-2018-7760

CISA Advisory Publication Process



Researcher discovers vulnerability

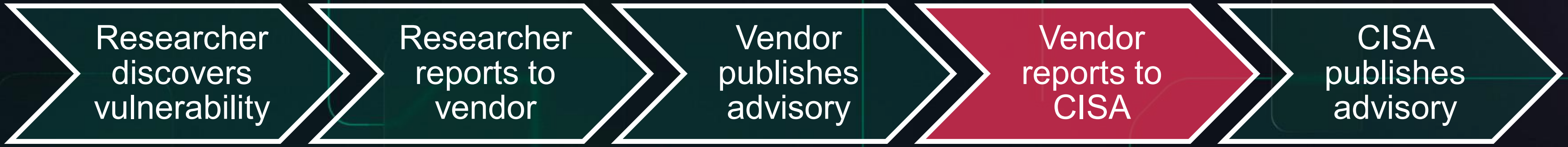
Researcher reports to vendor

Vendor publishes advisory

Vendor reports to CISA

CISA publishes advisory

CISA Advisory Publication Process



Researcher discovers vulnerability

Researcher reports to vendor

Vendor publishes advisory

Vendor reports to CISA

CISA publishes advisory

Old CISA Problem: Human-Readable Data

The following versions of Advantech WebAccess HMI Designer, a Human Machine Interface (HMI) runtime development software, are affected:

- Advantech WebAccess HMI Designer Version 2.1.9.23 and prior

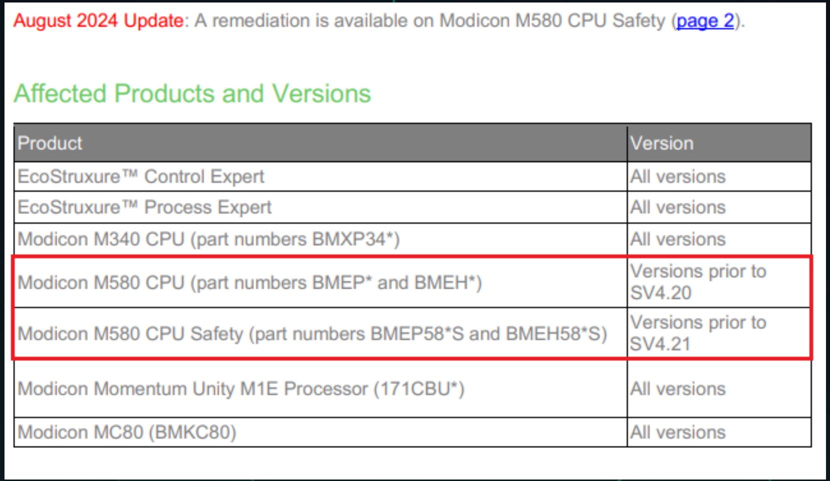
https://www.us-cert.gov/ics/advisories/icsa-19-213-01

CISA CSAF: Machine-Readable Data

```
"vulnerabilities": [
  {
    "cve": "CVE-2019-10961",
    "cwe": {
      "id": "CWE-787",
      "name": "Out-of-bounds Write"
    },
    ...
    "product_status": {
      "known_affected": [
        "CSAFPID-0001"
      ]
    },
    ...
  }
]
```

https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2019/icsa-19-213-01.json

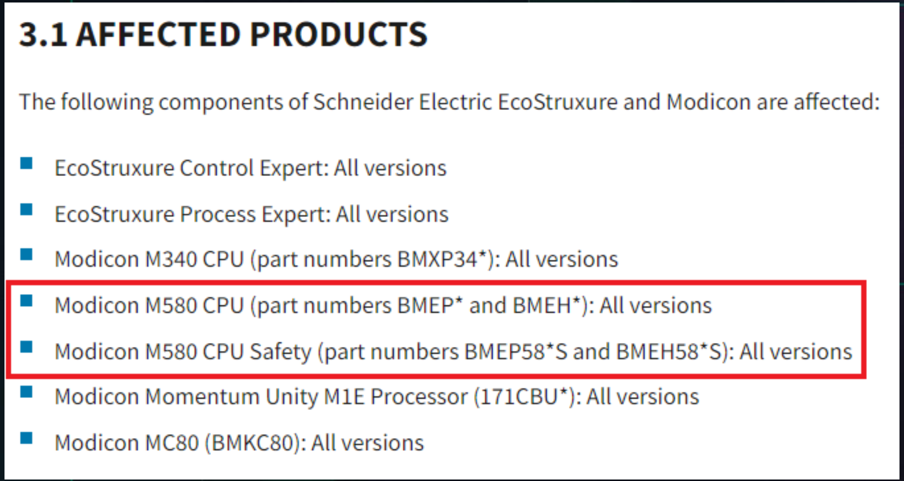
CISA: Missing updates



August 2024 Update: A remediation is available on Modicon M580 CPU Safety (page 2).

Affected Products and Versions

Product	Version
EcoStruxure™ Control Expert	All versions
EcoStruxure™ Process Expert	All versions
Modicon M340 CPU (part numbers BMXP34*)	All versions
Modicon M580 CPU (part numbers BMEP* and BMEH*)	Versions prior to SV4.20
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S)	Versions prior to SV4.21
Modicon Momentum Unity M1E Processor (171CBU*)	All versions
Modicon MC80 (BMKC80)	All versions



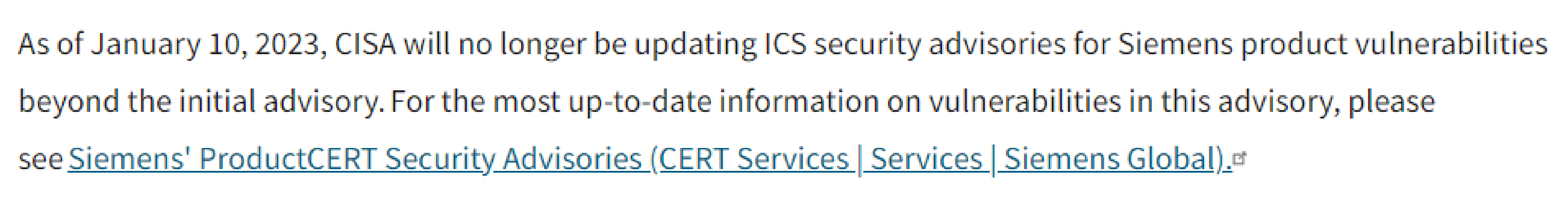
3.1 AFFECTED PRODUCTS

The following components of Schneider Electric EcoStruxure and Modicon are affected:

- EcoStruxure Control Expert: All versions
- EcoStruxure Process Expert: All versions
- Modicon M340 CPU (part numbers BMXP34*): All versions
- Modicon M580 CPU (part numbers BMEP* and BMEH*): All versions
- Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S): All versions
- Modicon Momentum Unity M1E Processor (171CBU*): All versions
- Modicon MC80 (BMKC80): All versions

- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-010-06&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-010-06_Modicon_Controllers_Security_Notification.pdf
- https://www.cisa.gov/news-events/ics-advisories/icsa-23-227-01

CISA stopped tracking updates for Siemens advisories



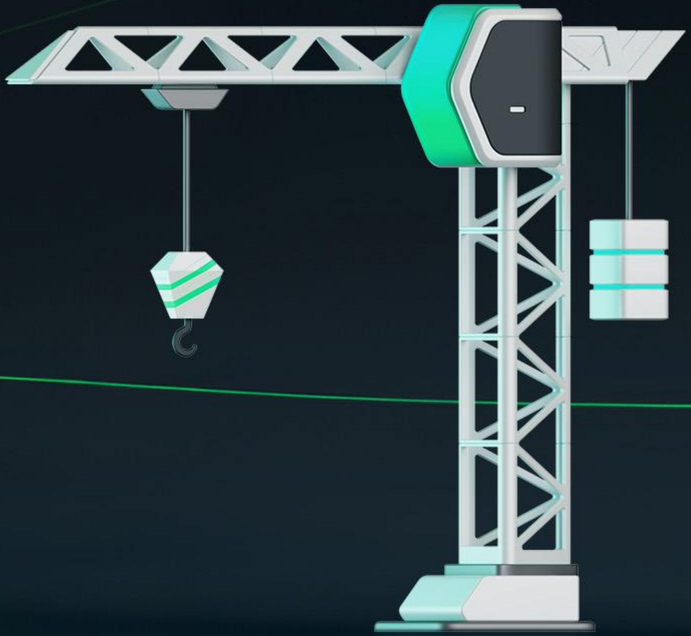
As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory. For the most up-to-date information on vulnerabilities in this advisory, please see Siemens' ProductCERT Security Advisories (CERT Services | Services | Siemens Global).

Problems

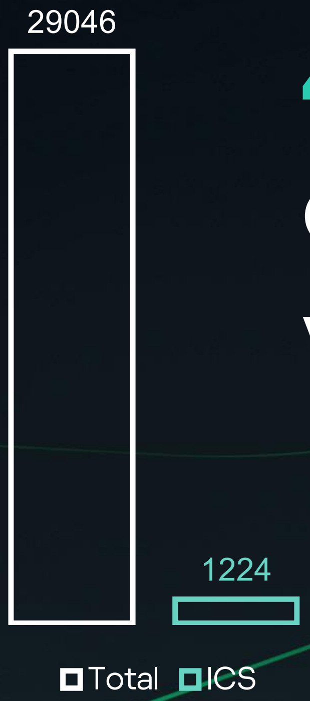
- Amount of data
- Human-readable data (for old vulnerabilities)
- Missing updates

CVE Project (ex-MITRE)

CVE®

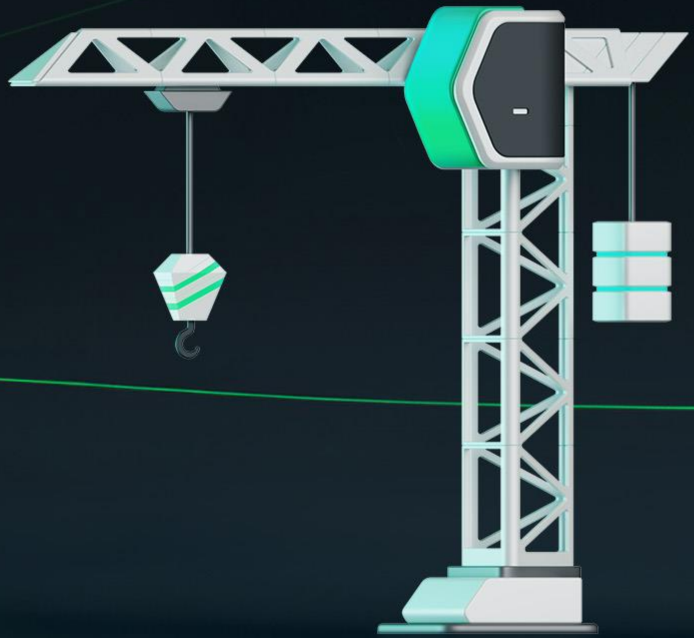


CVE Project: ICS Vulnerabilities

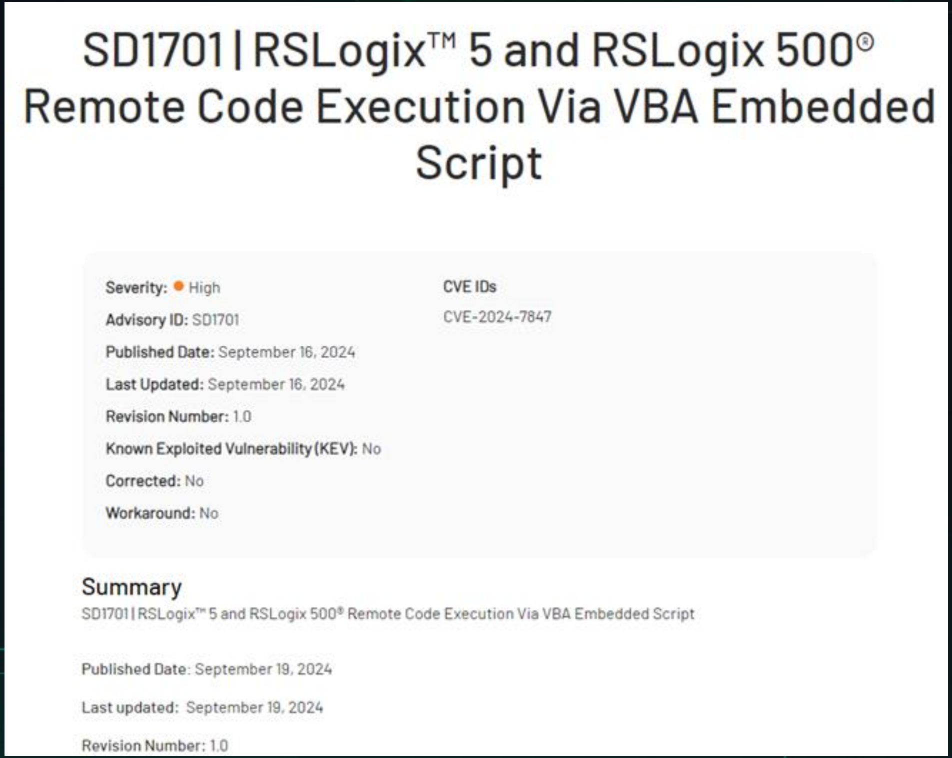


4%

of all vulnerabilities



CVE Project: Missing Information



SD1701 | RSLogix™ 5 and RSLogix 500® Remote Code Execution Via VBA Embedded Script

Severity: ● High

Advisory ID: SD1701

Published Date: September 16, 2024

Last Updated: September 16, 2024

Revision Number: 1.0

Known Exploited Vulnerability (KEV): No

Corrected: No

Workaround: No

CVE IDs

CVE-2024-7847

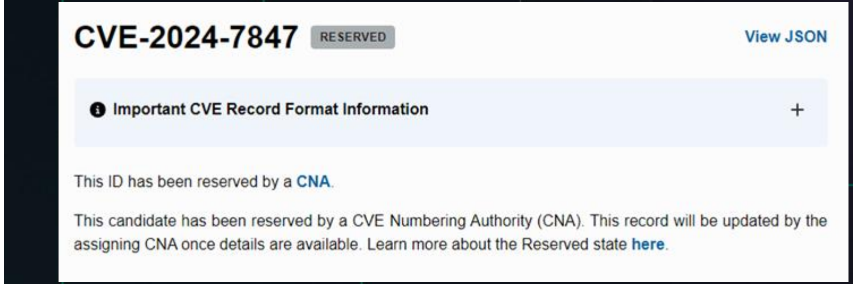
Summary

SD1701 | RSLogix™ 5 and RSLogix 500® Remote Code Execution Via VBA Embedded Script

Published Date: September 19, 2024

Last updated: September 19, 2024

Revision Number: 1.0



CVE-2024-7847 RESERVED

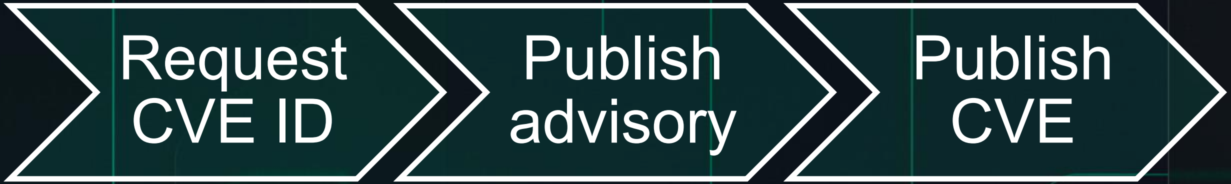
Important CVE Record Format Information +

This ID has been reserved by a **CNA**.

This candidate has been reserved by a CVE Numbering Authority (CNA). This record will be updated by the assigning CNA once details are available. Learn more about the Reserved state **here**.

- https://www.rockwellautomation.com/en-ch/trust-center/security-advisories/advisory.SD1701.html
- https://www.cve.org/CVERecord?id=CVE-2024-7847

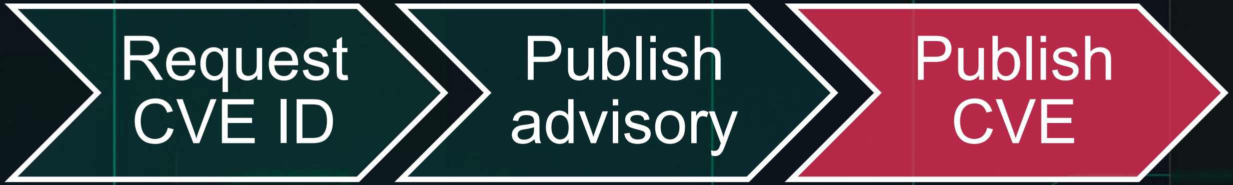
CVE Publication Process


Request CVE ID

Publish advisory

Publish CVE

CVE Publication Process

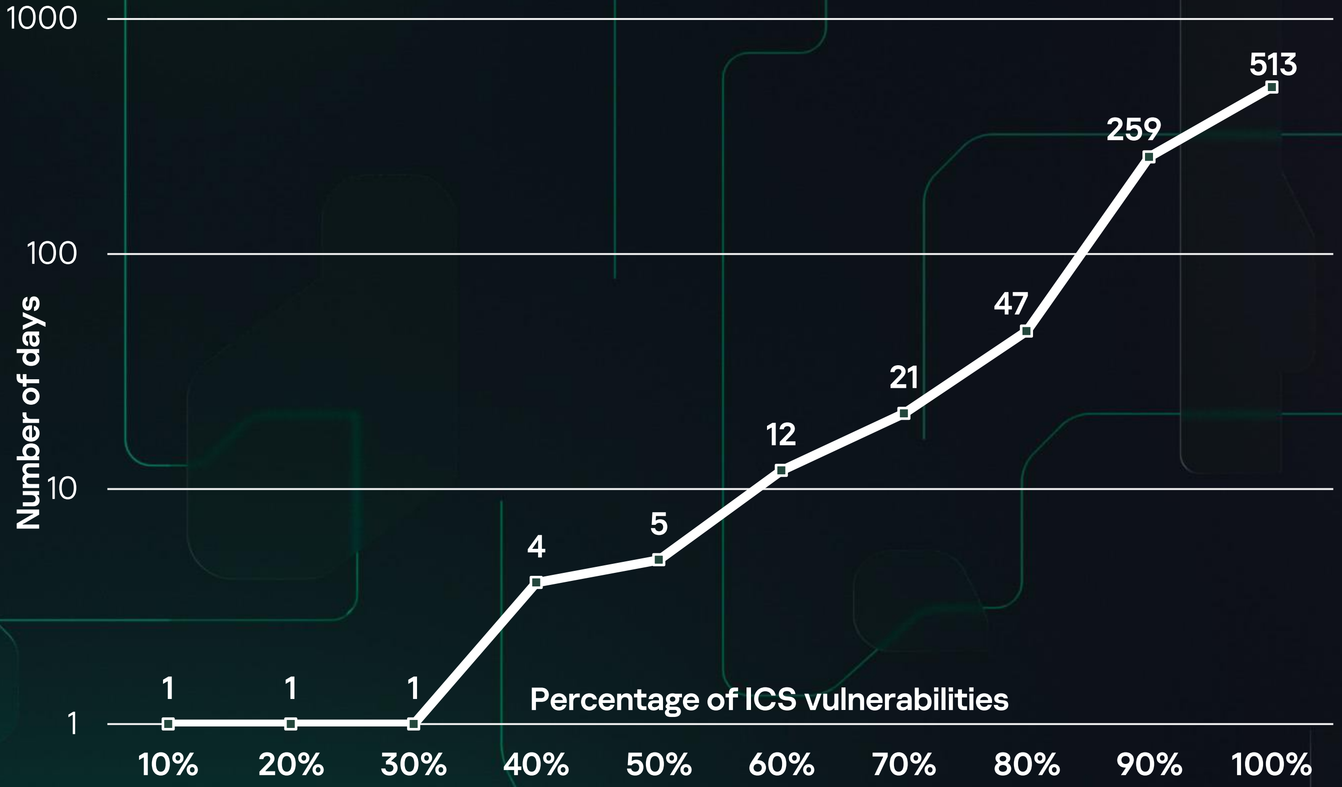


Request CVE ID

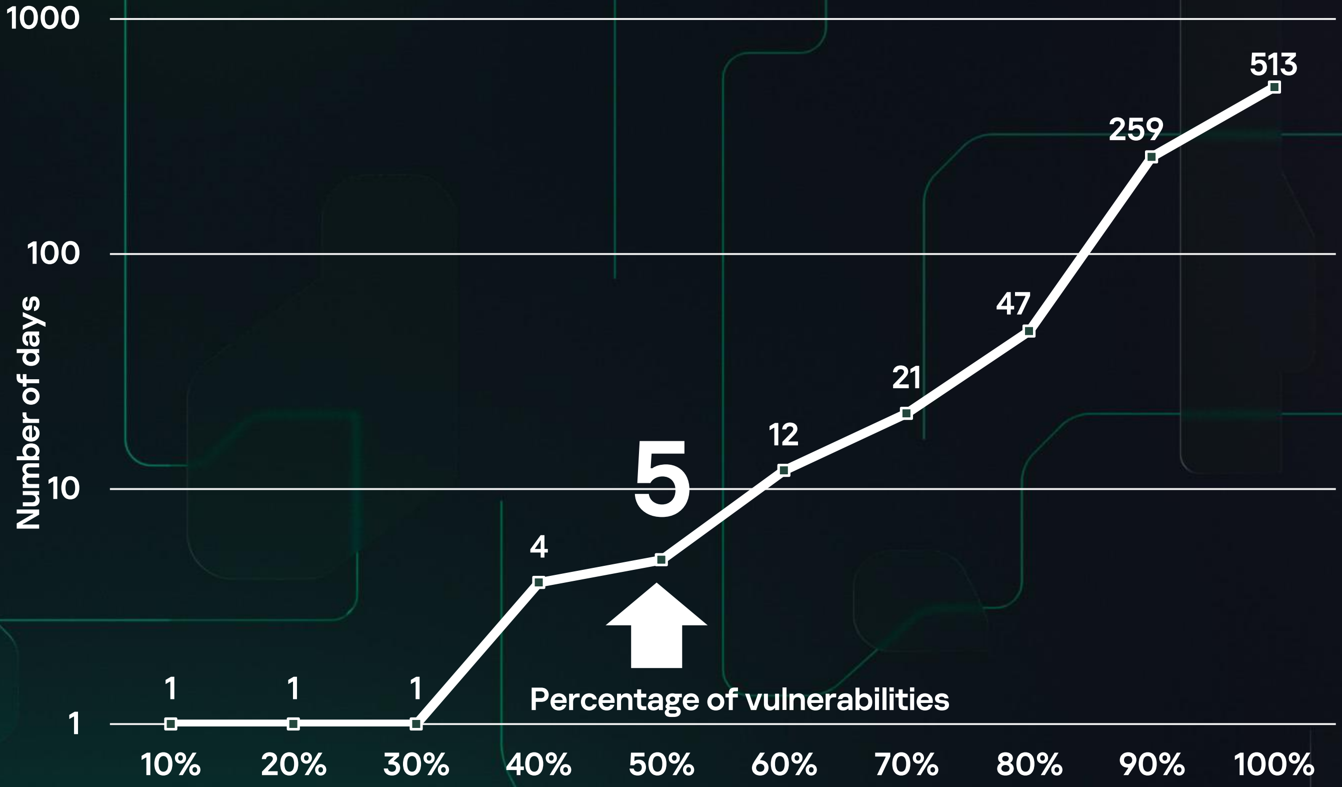
Publish advisory

Publish CVE

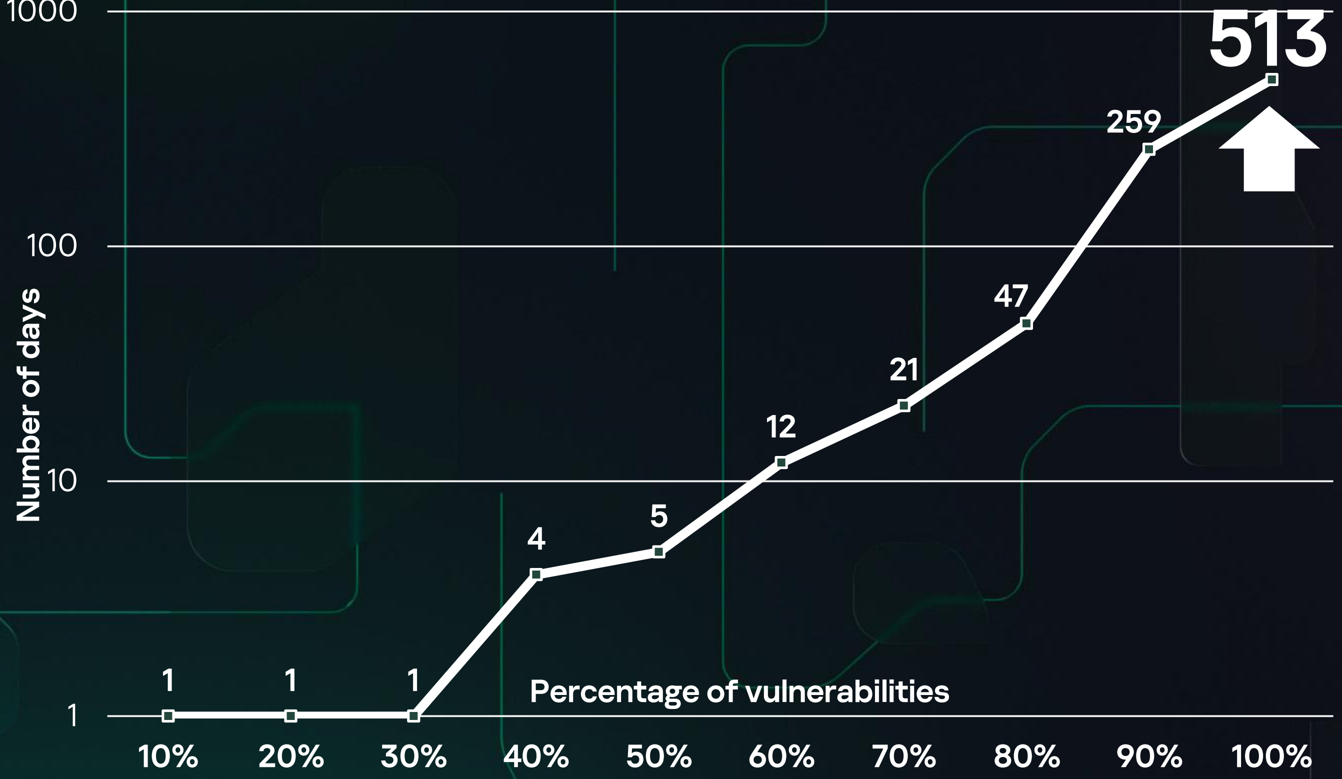
CVE Project: Delay



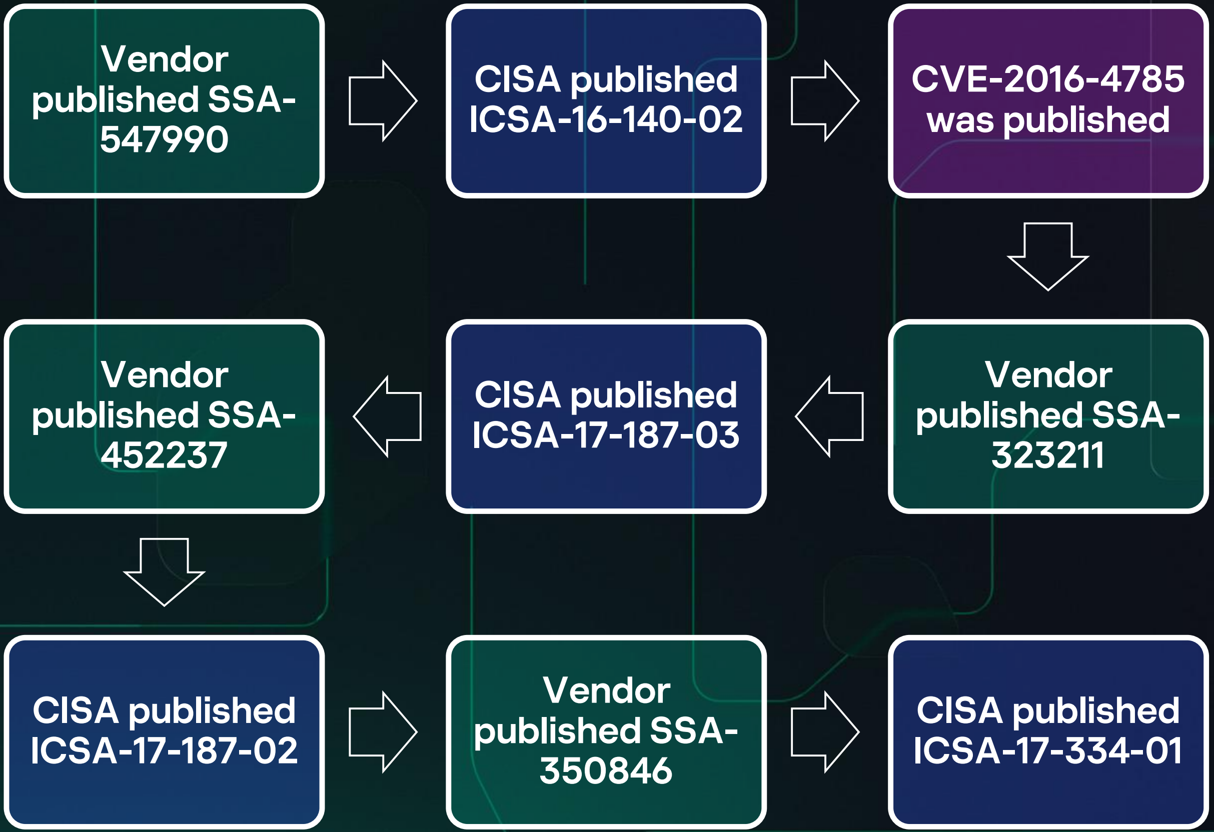
CVE Project: Delay



CVE Project: Delay



CVE Project: CISA Advisory Publication Process



Vendor published SSA-547990

CISA published ICSA-16-140-02

CVE-2016-4785 was published

Vendor published SSA-323211

CISA published ICSA-17-187-03

Vendor published SSA-452237

CISA published ICSA-17-187-02

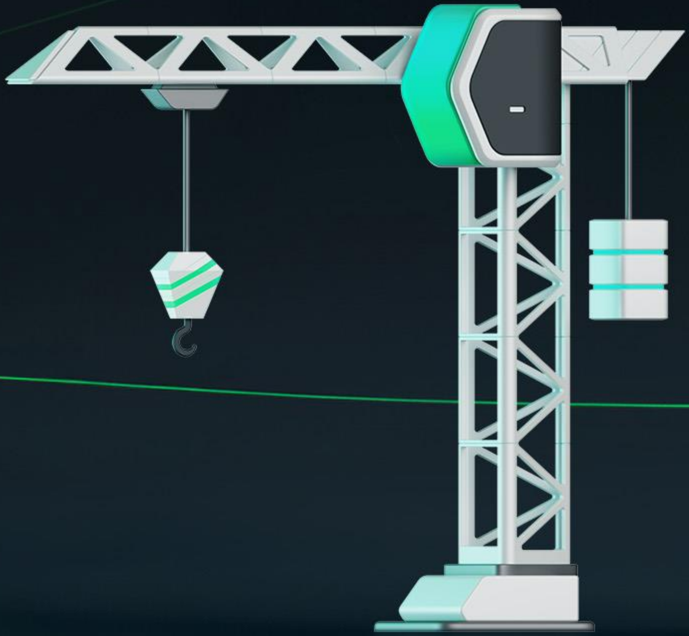
Vendor published SSA-350846

CISA published ICSA-17-334-01

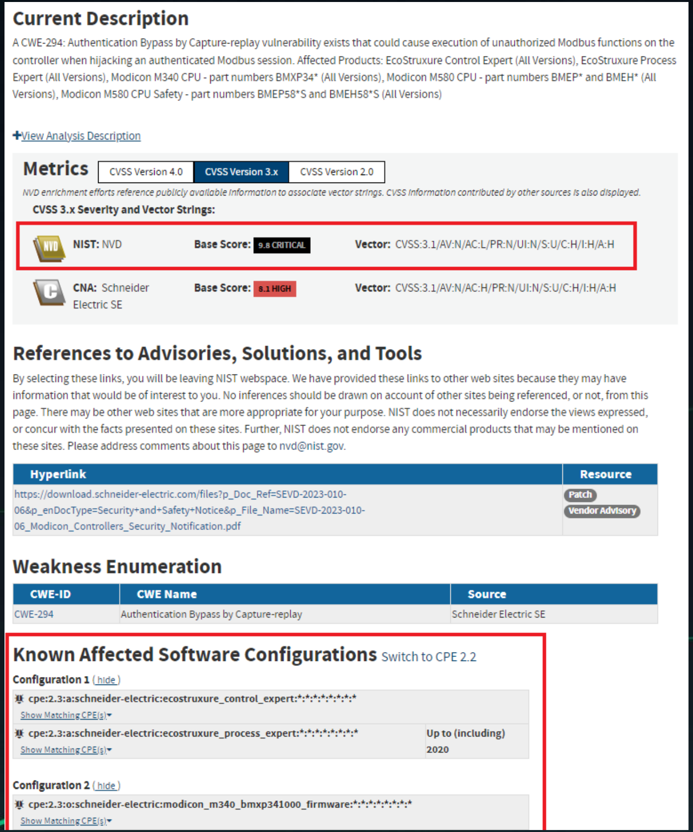
Problems

- Need to filter ICS vulnerabilities
- Delay
- Missing vulnerabilities
- Missing updates

NVD (National Vulnerability Database)



NVD: Information Enrichment



Current Description

A CWE-294: Authentication Bypass by Capture-replay vulnerability exists that could cause execution of unauthorized Modbus functions on the controller when hijacking an authenticated Modbus session. Affected Products: EcoStruxure Control Expert (All Versions), EcoStruxure Process Expert (All Versions), Modicon M340 CPU - part numbers BMXP34* (All Versions), Modicon M580 CPU - part numbers BMEP* and BMEH* (All Versions), Modicon M580 CPU Safety - part numbers BMEP58*S and BMEH58*S (All Versions)

+View Analysis Description

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CNA: Schneider Electric SE **Base Score:** 8.1 HIGH **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-010-06&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-010-06_Modicon_Controllers_Security_Notification.pdf	Patch Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-294	Authentication Bypass by Capture-replay	Schneider Electric SE

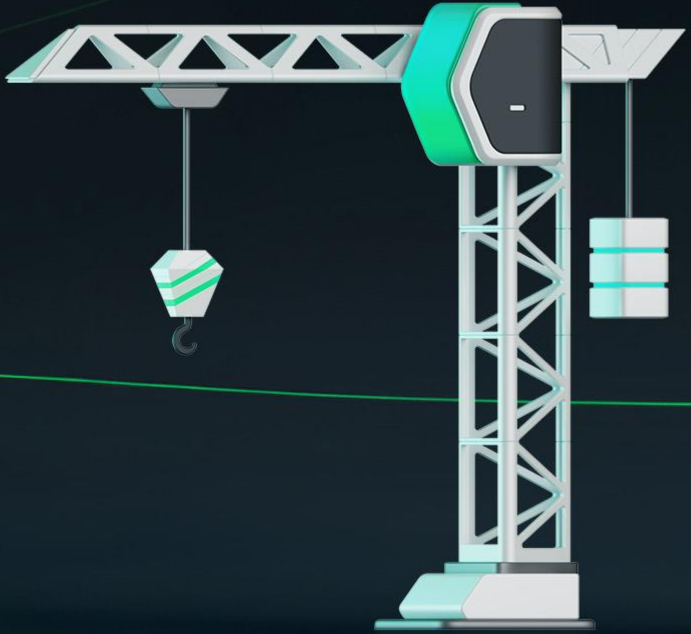
Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:schneider-electric:ecostruxure_control_expert:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	
cpe:2.3:a:schneider-electric:ecostruxure_process_expert:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	Up to (including) 2020

Configuration 2 (hide)

cpe:2.3:o:schneider-electric:modicon_m340_bmxp341000_firmware:*:*:*:*:*:*:*:* Show Matching CPE(s)▾



https://nvd.nist.gov/vuln/detail/CVE-2022-45789

NVD: Machine-Readable Data

```
cpe:2.3:a:siemens:simatic_pcs_7:8.0:*:*:*:*:*:*:*
cpe:2.3:a:siemens:simatic_pcs_7:8.1:*:*:*:*:*:*:*
cpe:2.3:a:siemens:simatic_pcs_7:8.2:*:*:*:*:*:*:*
cpe:2.3:a:siemens:simatic_pcs_7:9.0:*:*:*:*:*:*:*
```

https://nvd.nist.gov/vuln/detail/CVE-2019-10935

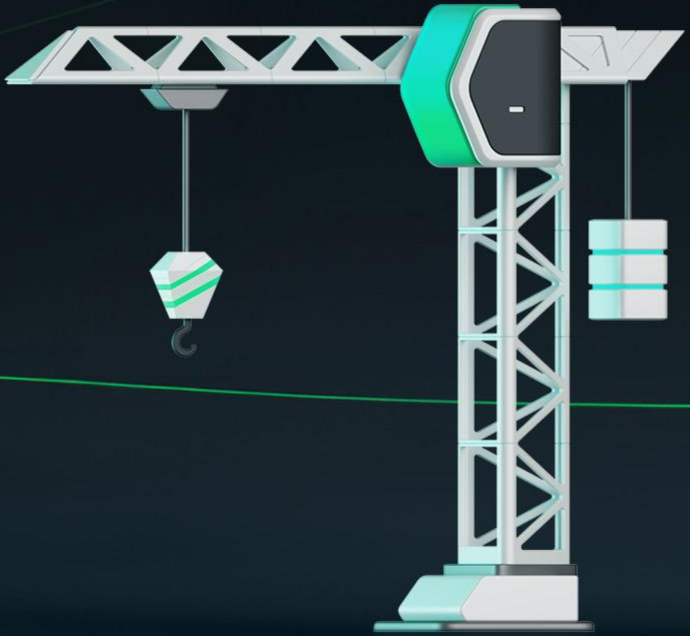
Problems

- Delay
- Need to filter ICS vulnerabilities
- Missing vulnerabilities
- Missing updates

Problems

- Delay
- Need to filter ICS vulnerabilities
- Missing vulnerabilities
- Missing updates and **enrichment errors**

Errors



Errors: SEVD-2019-134-11 (CVE-2018-7854)

A CWE-248 Uncaught Exception vulnerability exists which could cause a denial of service when sending invalid debug parameters to the controller over Modbus.

https://www.se.com/ww/en/download/document/SEVD-2019-134-11/

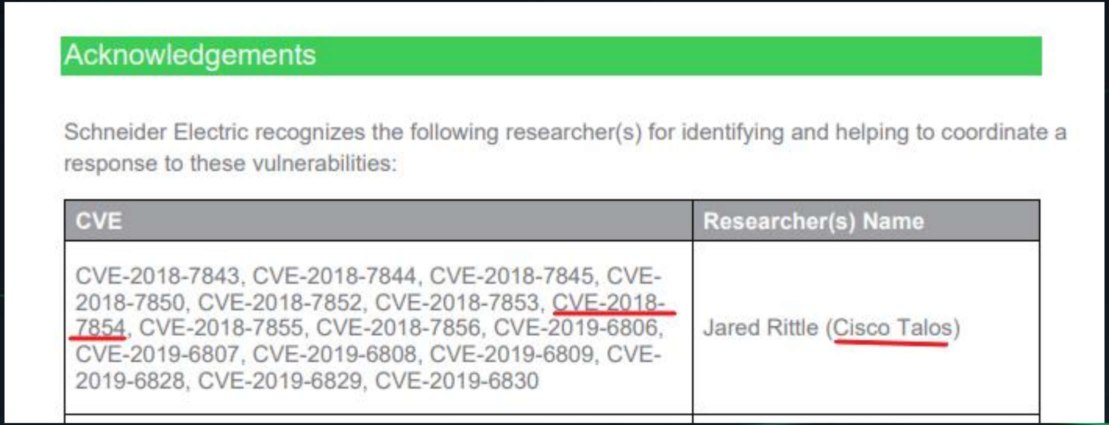
Errors: SEVD-2019-134-11 (CVE-2018-7854)

CVSSv3 Base Score: **7.5 (High)**

AV:N/AC:L/**PR:N**/UI:N/S:U/C:N/I:N/**A:H**

https://www.se.com/ww/en/download/document/SEVD-2019-134-11/

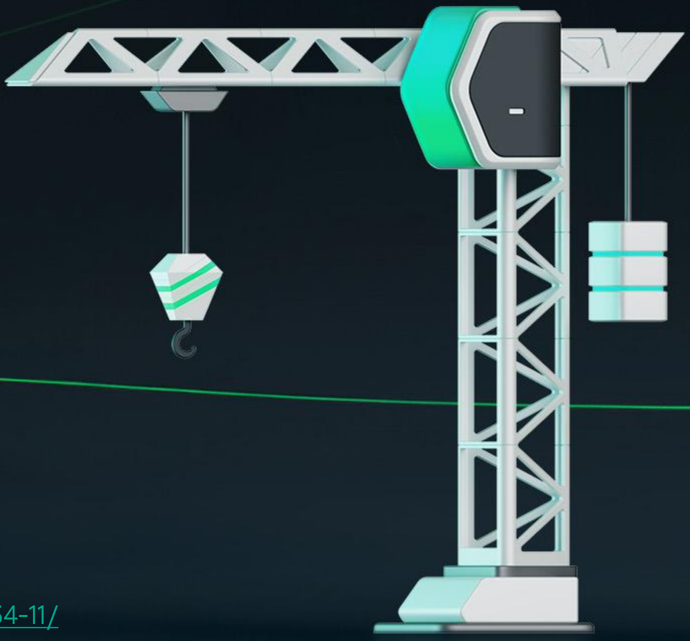
Errors: SEVD-2019-134-11 (CVE-2018-7854)



Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher(s) Name
CVE-2018-7843, CVE-2018-7844, CVE-2018-7845, CVE-2018-7850, CVE-2018-7852, CVE-2018-7853, CVE-2018-7854, CVE-2018-7855, CVE-2018-7856, CVE-2019-6806, CVE-2019-6807, CVE-2019-6808, CVE-2019-6809, CVE-2019-6828, CVE-2019-6829, CVE-2019-6830	Jared Rittle (Cisco Talos)



https://www.se.com/ww/en/download/document/SEVD-2019-134-11/

Errors: TALOS-2019-0765

This can be completed by first obtaining a **PLC reservation**, and then sending a data payload …

https://talosintelligence.com/vulnerability_reports/TALOS-2019-0765

Errors: SEVD-2019-134-11 (CVE-2018-7854)

Privileges Required: **None** -> **High**

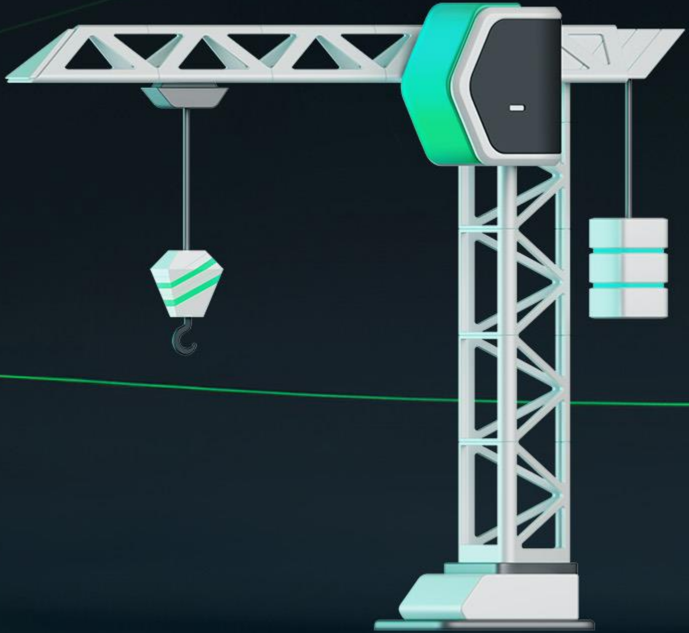
Errors: SEVD-2019-134-11 (CVE-2018-7854)

Privileges Required: **None** -> **High**

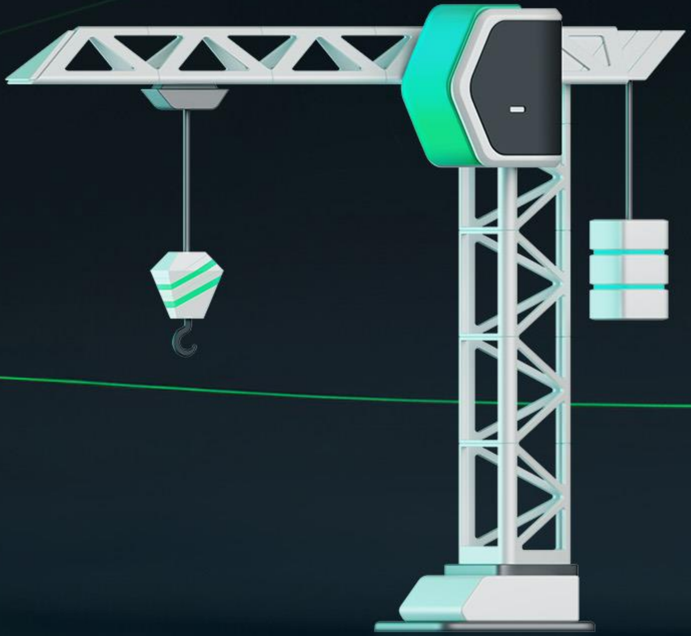
Availability: **High** -> **None**

CVSSv3 Base Score: **0.0 (None)**

Errors: SEVD-2019-134-11 (CVE-2018-7854)



78% ICS vulns with errors



Recommendations

- Monitor all information sources
- Perform a vulnerability analysis
- Staff trainings

Thank you!

https://ics-cert.kaspersky.com

Artem Zinenko

Head of ICS CERT Vulnerability
Research and Assessment

Artem.Zinenko@kaspersky.com

kaspersky

ICS
CERT