

Enhancing Cyber Resilience: CSAF + VEX

Justin Murphy
April 12, 2024



Justin Murphy
April 12, 2024

whoami

Justin Murphy

Vulnerability Analyst: CVD Team @CISA

Passion for:

- Service
- International Cooperation
- Coordinated Vulnerability Disclosure (CVD)
- Vulnerability Management/Supply Chain Transparency
- CSAF/OpenEoX
- SBOM/VEX



Justin Murphy
April 12, 2024

Common Security Advisory Framework (CSAF)

International, open and free OASIS standard

Machine-readable format for security advisories (JSON) and VEX

Standardized way for distribution of security advisories

Build with automation in mind

Standardized tool set

Guidance to actionable information

CSAF allows for linking to SBOM data.

Successor of CVRF 1.2



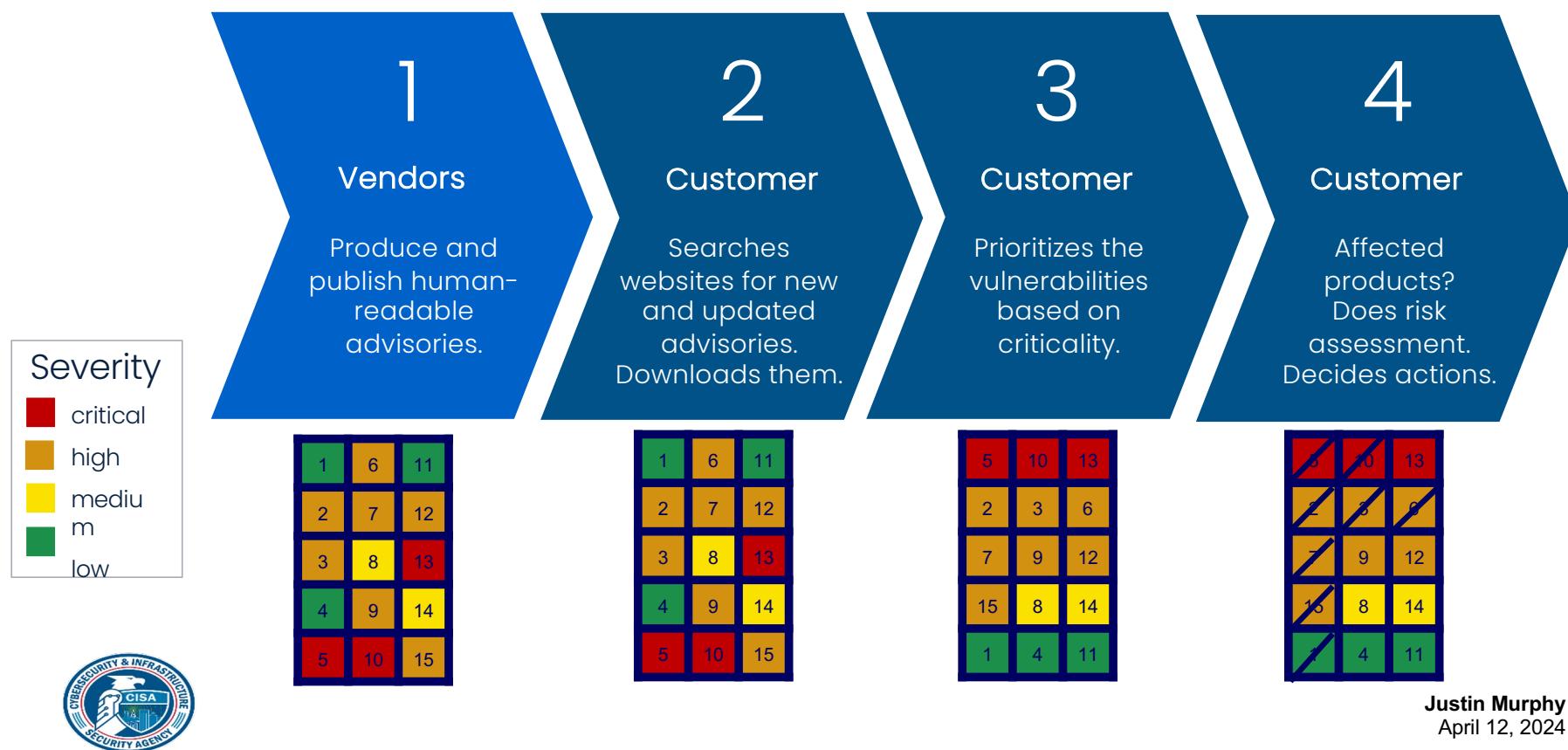
Justin Murphy
April 12, 2024

Log | Shell™

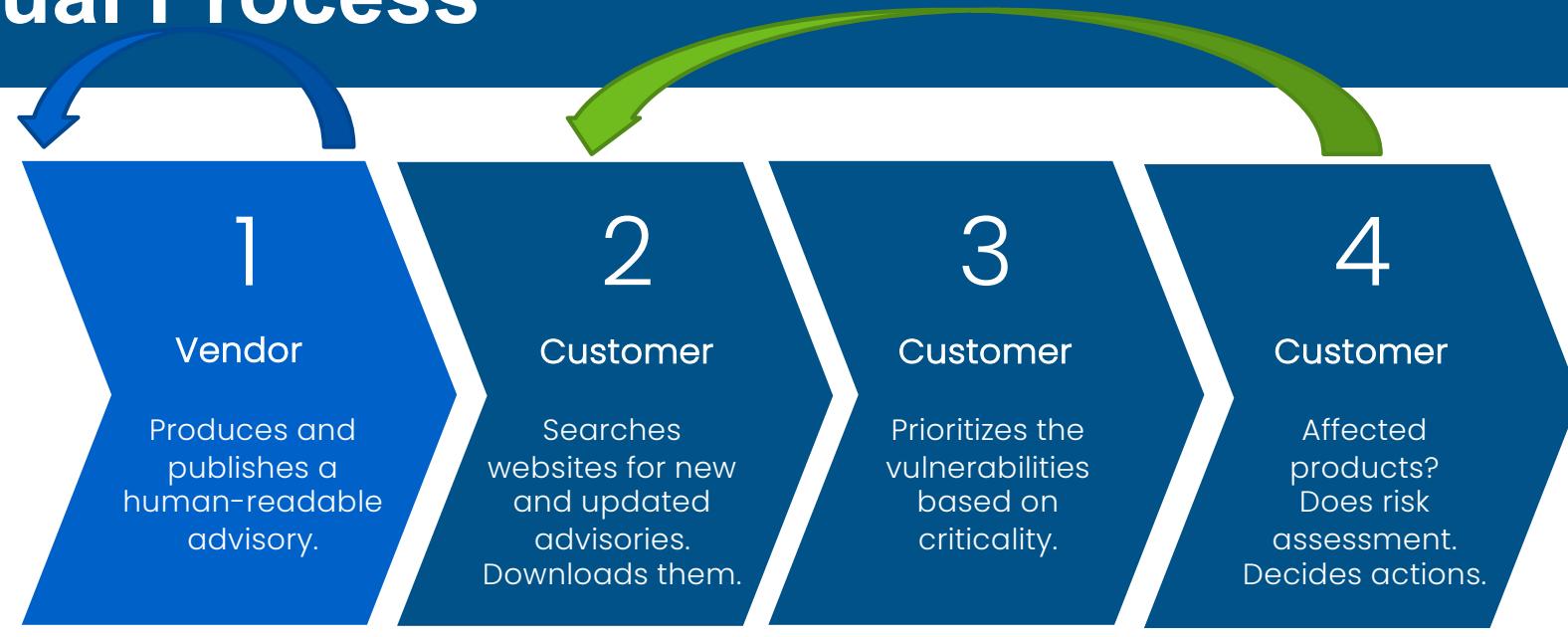


Justin Murphy
April 12, 2024

Manual Process



Manual Process



Severity

- critical
- high
- medium
- low

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

5	10	13
2	3	6
7	9	12
15	8	14
1	4	11

6	10	13
2	3	9
7	9	12
16	8	14
4	11	



Justin Murphy
April 12, 2024

SIEMENS

[Subscribe to Security Advisories](#)

Search Security Advisories

Search (SSA-ID, CVE-ID, Title, Products, Sector, Tag)

Filter by Date | Reset

ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-822830	7.8	Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V15.1.0	View	V1.2	2021-05-17	PDF TXT
SSA-663999	7.8	Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V15.1.0.1	View	V1.1	2021-05-17	PDF TXT
SSA-695540	7.8	ASM and PMR File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V15.1.0.2	View	V1.0	2021-05-17	PDF TXT
SSA-116379	7.5	Denial-of-Service Vulnerability in OSPF Packet Handling of SCALANCE XM-400 and XM-500 Devices	View	V1.0	2021-05-11	PDF TXT
SSA-208838	9.8	Multiple Vulnerabilities in SINAMICS Medium Voltage Products	View	V1.0	2021-05-11	PDF TXT
SSA-324955	7.4	SAD DNS Attack in Linux Based Products	View	V1.0	2021-05-11	PDF TXT
SSA-501075	7.8	Vulnerabilities in Controllers CPU 1510 MTF using Intel CPUs (November 2020)	View	V1.0	2021-05-11	PDF TXT
SSA-558770	9.8	SmartWNC Vulnerabilities in SIMATIC HMI/WinCC Products	View	V1.0	2021-05-11	PDF TXT
SSA-594264	5.3	Denial-of-Service Vulnerability in SNMP Implementation of WinCC Runtime	View	V1.0	2021-05-11	PDF TXT
SSA-679775	7.5	Denial-of-Service Vulnerability in SIMATIC NET CP 343-1 Devices	View	V1.0	2021-05-11	PDF TXT
SSA-679893	7.8	Vulnerabilities in Industrial PCs and CNC devices using Intel CPUs (November 2020)	View	V1.0	2021-05-11	PDF TXT
SSA-723417	9.8	Multiple Vulnerabilities in SCALANCE W17500	View	V1.0	2021-05-11	PDF TXT
SSA-752103	8.1	Telnet Authentication Vulnerability in SINAMICS Medium Voltage Products	View	V1.0	2021-05-11	PDF TXT



Justin Murphy
April 12, 2024

Technology & Innovation Cyber security Cyber security alerts and notifications

Cyber security alerts and notifications

We are committed to providing our customers with products, systems and services that clearly address cyber security. Proper and timely handling of cyber security incidents and software vulnerabilities is one important factor in helping our customers minimize risks associated with cyber security.

[Latest](#) [Archived](#) [Subscribe to email alerts](#) [Report vulnerability](#)

2021

- [2021-05-06: Cybersecurity Advisory - AC 800PEC platform NAME-WRECK vulnerability](#)
- [2021-05-06: Cybersecurity Advisory - Cassia Access Controller for ABB](#)
- [2021-04-30: Cybersecurity Advisory - Denial-of-service vulnerability affecting multiple B&R products](#)
- [2021-02-12: Cybersecurity Advisory - CodeMeter Vulnerabilities, Impact on B&R products](#)
- [2021-02-02: Cybersecurity Advisory - AC500 V2 Webserver vulnerability](#)



Justin Murphy
April 12, 2024

SIEMENS						
Search Security Advisories						
<input type="text" value="Search (SA-1, CSF-0, Title, Product, Series, Tag)"/> Filter by Date Reset						
ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-622130	7.8	Multiple File Parsing Vulnerabilities in J2Go and Teamcenter Visualization before V13.1.0	View	V1.2	2021-05-17	PDF TXT
SSA-663199	7.8	Multiple File Parsing Vulnerabilities in J2Go and Teamcenter Visualization before V13.1.0.1	View	V1.1	2021-05-17	PDF TXT
SSA-695540	7.8	ASW and INI File Parsing Vulnerabilities in J2Go and Teamcenter Visualization before V13.1.0.2	View	V1.0	2021-05-17	PDF TXT
SSA-116179	7.5	Denial-of-Service Vulnerability in CSFF Packet Handling of SCALANCE XM-400 and XM-500 Devices	View	V1.0	2021-05-11	PDF TXT
SSA-200130	9.8	Multiple Vulnerabilities in SIMATIC Medium Voltage Products	View	V1.0	2021-05-11	PDF TXT
SSA-324155	7.4	SAD DNS Attack in Linux-based Products	View	V1.0	2021-05-11	PDF TXT
SSA-501073	7.8	Vulnerabilities in Controllers CPU 1510 MTP using Intel CPUs (November 2020)	View	V1.0	2021-05-11	PDF TXT
SSA-558770	9.8	SmartWNC Vulnerabilities in SIMATIC HMI/SIMATIC Products	View	V1.0	2021-05-11	PDF TXT
SSA-594264	5.3	Denial-of-service Vulnerability in SNMP Implementation of WinCC Runtime	View	V1.0	2021-05-11	PDF TXT
SSA-678775	7.5	Denial-of-Service Vulnerability in SIMATIC NET CP 343-1 Devices	View	V1.0	2021-05-11	PDF TXT
SSA-678483	7.8	Vulnerabilities in Industrial PCs and CNC devices using Intel CPUs (November 2020)	View	V1.0	2021-05-11	PDF TXT
SSA-723117	9.8	Multiple Vulnerabilities in SCALANCE WI-7500	View	V1.0	2021-05-11	PDF TXT
SSA-752103	8.1	Ticket Authentication Vulnerability in SIMATIC Medium Voltage Products	View	V1.0	2021-05-11	PDF CSV

ABB

Cybersecurity notifications

We are committed to providing you with the latest information and services related to the handling of cybersecurity threats. We are one of the most important companies associated with ABB.

Latest news

2021

2021-05-06: Cybersecurity Advisory - AC 800PEC platform NAME:WRECK vulnerability

2021-05-06: Cybersecurity Advisory - Cassia Access Controller for ABB

2021-04-30: Cybersecurity Advisory - Denial-of-service vulnerability affecting multiple B&R products

2021-02-12: Cybersecurity Advisory - CodeMeter Vulnerabilities, Impact on B&R products

2021-02-02: Cybersecurity Advisory - AC500 V2 Webserver vulnerability

PRODUCT SUPPORT

Security Advisories

Industrial Cybersecurity

As adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of our top priorities. Our Security Response Team (CSRT) is taking a proactive approach to protect our products from security risks. We are committed to managing security risks.

Check Moxa's Product Security Advisories

Our security advisories include details of our product vulnerabilities as well as the solutions available.

Subscribe to Moxa's Security Advisories

Subscribe to our security advisories to receive the latest vulnerability information about our products.

Moxa's Response Regarding Sudo Heap-based Buffer Overflow Vulnerability (CVE-2021-3156)

Recently Released

NAME	LAST UPDATED
NPort IA500A Series Serial Device Servers Vulnerabilities	Apr 26, 2021
EDR ero Sensors Security Router Vulnerabilities	Mar 23, 2021
VPoint IEEE 802.3af PoE IP Camera Vulnerabilities	Mar 16, 2021
Moxa's Response Regarding Sudo Heap-based Buffer Overflow Vulnerability (CVE-2021-3156)	Feb 17, 2021

SIEMENS

Search Security Advisories

Search (SIA-E, CAA-I, TIA4, Proactive, Service, Tag) Filter by Date Reset

Subscribe to Security Advisories

Info	Version	Last Update	Download
Issues in JT2Go and Teamcenter Visualization before V1.3.1.0	V1.2	2021-05-17	PDF TXT
Issues in JT2Go and Teamcenter Visualization before V1.3.1.0.1	V1.1	2021-05-17	PDF TXT
Issues in JT2Go and Teamcenter Visualization before V1.3.1.0.2	V1.0	2021-05-17	PDF TXT
SPF Packet Handling of SCALANCE XM-400 and XM-500	V1.0	2021-05-11	PDF TXT
3 Medium Voltage Products	V1.0	2021-05-11	PDF TXT
Issues	V1.0	2021-05-11	PDF TXT
S10 MFP using Intel CPUs (November 2020)	V1.0	2021-05-11	PDF TXT
IC-HMI/SIMATIC Products	V1.0	2021-05-11	PDF TXT
NMP Implementation of WiFi6C Runtimes	V1.0	2021-05-11	PDF TXT
INMATIC NET CP 343-1 Devices	V1.0	2021-05-11	PDF TXT
T-Line devices using Intel CPUs (November 2020)	V1.0	2021-05-11	PDF TXT
CE WI-7500	V1.0	2021-05-11	PDF TXT
Issues in SIMATIC Medium Voltage Products	V1.0	2021-05-11	PDF TXT

Justin Murphy
April 12, 2024

Bosch PSIRT Security Advisories

Siemens

VDE CERT

ABB

Siemens

e Engineering Institute

Pepperl+Fuchs

ICS-CERT Advisories

CISA

April 12, 2022

The collage illustrates the complex landscape of industrial cybersecurity, featuring:

- Westermo**: A screenshot showing a 'Security Notifications' page with a table of recent vulnerabilities.
- Bosch**: The 'Bosch PSIRT Security Advisories' page, which lists security advisories for Bosch products, categorized by year (2021, 2020, 2019) and type (Security Advisory, Security Response).
- Siemens**: The 'Search Security Advisories' page, displaying a grid of security advisories from Siemens, including details like 'Serial', 'Last Updated', and 'Affected Bosch Products'.
- Sprecher**: A screenshot of the 'Engineering Institute' section, showing a 'Vulnerability Notes Database' and a 'SECURITY ALERTS' section.
- VDE CERT**: The 'Advisories' page, listing various security bulletins and notifications.
- ABB**: The 'Cyber security notifications' page, showing a table of recently released notifications.
- JP CERT**: A screenshot of the 'Cybersecurity Information and Reporting' section, featuring a banner about 'Towards a digital cyber zone in our industries'.
- Pepperl+Fuchs**: The 'Cyber Security Information and Reporting' page, with a prominent 'Report a vulnerability to the Pepperl+Fuchs CERT' button.



Automation?

April 12, 2022

An official website of the United States government Here's how you know 



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



Search Services Resources

Alerts and Tips Resources Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

ICS Advisory (ICSA-21-138-01)

Emerson Rosemount X-STREAM

Original release date: May 18, 2021

 Print  Tweet  Send  Share

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of a regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Light Protocol (TLP) marking in the header. For more information about TLP, see <https://us-cert.cisa.gov/tlp/>.

1. EXECUTIVE SUMMARY

- **CVSS v3.7.5**
- **ATTENTION:** Exploitable remotely/low attack complexity
- Vendor: Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS





-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE W1700 Devices

Publication Date:	2019-12-10
Last Update:	2019-12-10
Current Version:	v1.0
CVSS v3.1 Base Score:	6.5

SUMMARY
=====

The latest firmware updates for the SCALANCE W700 and W1700 wireless device families fix a vulnerability affecting WPA/WPA2 key handling. It might be possible to, by manipulating the EAPO-LKey frames, decrypt the Key Data field without the frame being authenticated.

This has impact on WPA/WPA2 architectures using TKIP encryption. The attacker must be in the wireless range of the device to perform the attack.

AFFECTED PRODUCTS AND SOLUTION
=====

- * SCALANCE W1700
 - Affected versions:
All versions < V1.1
 - Remediation:
Update to V1.1 or any later version
 - Download:
<https://support.industry.siemens.com/cs/wv/en/view/109762253>
- * SCALANCE W700
 - Affected versions:
All versions < V6.4
 - Remediation:
Update to V6.4 or any later version
 - Download:
<https://support.industry.siemens.com/cs/wv/en/view/109773308>

WORKAROUNDS AND MITIGATIONS
=====

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- * Whenever possible, use AES-CMP instead of TKIP in the WPA/WPA2 networks. This can be configured for both SCALANCE W-700 and W-1700 families over the Web Based Management (web server). For more information, go for the respective Manual.

GENERAL SECURITY RECOMMENDATIONS
=====

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download:
<https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.

Justin Murphy
April 12, 2024

An official website of the United States government Here's how you know 

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search Services Requests

Alerts and Tips Resources Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

ICS Advisory (ICSA-21-13)

Emerson Rosemount X-STREAM

Original release date: May 18, 2021

 Print Tweet Send Share

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics/cert-advisories/icsa-21-13> are provided "as is" without warranty of any kind. The Department of Homeland Security (DHS) does not provide any warranties of a general nature (including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose) with respect to the information products contained in this product or otherwise. Further dissemination of this product is governed by the DHS Light Protocol (LTP) marking in the header. For more information, see the DHS LTP marking in the header.

1. EXECUTIVE SUMMARY

- **CVSS v3.7.5**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS



Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert

11 May 2021

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA). The [EcoStruxure Geo SCADA Expert](#) product is an open, flexible and scalable software system for telemetry and remote control of industrial assets.

Failure to apply the recommended patch may risk the revealing of account credentials, which could result in unauthorized access to the system.

Affected Products

- ClearSCADA
- EcoStruxure Geo SCADA Expert
- EcoStruxure Geo SCADA Expert (Historian)

Vulnerability Details

CVE ID: CVE-2021-2253
 CVSS v3.1 Base Score: 8.1 (High) - CVSS v2.0: 7.0 (High)
 Impact: Confidentiality / Integrity / Availability
 CVSS v3.1 Subscore: PR:H/U/I/N/S/C/H/I/A/H
 A CWE-916: Use of Uncontrolled Input in a Configuration File vulnerability exists that could cause a denial of service condition when server database files are available. Exposure of these files to an attacker can make the system vulnerable to password decryption attacks. Note that ".sde" configuration export files do not contain user account password hashes.

Remediation

Geo SCADA Expert 2020 April 2021 (83.7787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here:
<https://projects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads>

Installation of new server software will require system restart or changeover of redundant servers. Consult the Release Notes and Resource Center for advice on the procedure.

Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure.

-----BEGIN PGP SIGNED MESSAGE-----
 Hash: SHA512
 # SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE W1700 Devices
 Publication Date: 2019-12-10
 Last Update: 2019-12-10
 Current Version: 1.0
 CVSS v3.1 Base Score: 8.5
SUMMARY
 ======
 The latest firmware updates for the SCALANCE W700 and W1700 wireless device families fix a vulnerability affecting WPA/WPA2 key handling. It might be possible to, by manipulating the EAPOL-Key frames, decrypt the Key Data field without having the correct authentication.
 This has impact on WiFi devices using TKIP encryption. The attacker must be in the vicinity of the device to perform the attack.
AFFECTED PRODUCTS AND VULNERABILITY
 ======

- * SCALANCE W1700
 - Affected versions: All versions < V1.0
 - Remediation: Update to V1.0
 - Download: <https://support.industry.siemens.com/cs/wv/en/view/109762253>
- * SCALANCE W700
 - Affected versions: All versions < V6.4
 - Remediation: Update to V6.4 or any later version
 - Download: <https://support.industry.siemens.com/cs/wv/en/view/109773308>

WORKAROUNDS AND MITIGATIONS
 ======

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- * Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2 networks. This can be configured for both SCALANCE W-700 and W-1700 families over the Web Based Management (web server). For more information, go for the respective Manual.

GENERAL SECURITY RECOMMENDATIONS
 ======

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.

Justin Murphy
 April 12, 2024

An official website of the United States government Here's how you know ▾



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search Services Requests

Alerts and Tips Resources Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

ICS Advisory (ICSA-21-13)

Emerson Rosemount X-STREAM

Original release date: May 18, 2021

Print Tweet Send Share

HTML

All information products included in https://us-cert.cisa.gov/ics/cert/icsa-21-13.html are provided "as is" without warranty of any kind. The Department of Homeland Security (DHS) does not provide any warranties of a regarding any information contained within. DHS does not endorse any of the products or services mentioned in this product or otherwise. Further dissemination of this product is governed by the Light Protocol (LPL) marking in the header. For more information, see the LPL marking in the header.

1. EXECUTIVE SUMMARY

- **CVSS v3.5**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information.

3. TECHNICAL DETAILS

3.1 Affected Products

Emerson Rosemount X-STREAM Gas Analyzer

CISA



Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert

11 May 2021

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA).

The [EcoStruxure Geo SCADA Expert](#) product is an open, flexible and scalable software system for telemetry and remote control.

Failure to apply the recommended configuration may risk the revealing of account credentials, which could result in unauthorized access.

Affected Products

- ClearSCADA
- EcoStruxure Geo SCADA Expert
- EcoStruxure SCADA Expert

Vulnerability Details

CVE ID: CVE-2022-2253

CVSS v3.1 Base Score: 7.8 (High)

A CWE-916: Use of Uncontrolled Input in a Cryptographic Computational Effort vulnerability exists that could cause an attacker to gain unauthorized access when server database files are available. Exposure of these files to an attacker can make the system vulnerable to password decryption attacks. Note that "sde" configuration export files do not contain user account

PDF

TXT

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE W1700 Devices

Publication Date: 2019-12-10
Last Update: 2019-12-10
Current Version: 1.0
CVSS v3.1 Base Score: 6.5

SUMMARY
=====

The latest firmware updates for the SCALANCE W700 and W1700 wireless device families fix a vulnerability affecting WPA/WPA2 key handling. It might be possible to, by manipulating the EAPOL-Key frames, decrypt the Key Data field without having the correct authentication key.

This has impact on WPA/WPA2. An attacker must be in the same network as the device to perform the attack.

AFFECTED PRODUCTS AND VULNERABILITIES
=====

- * SCALANCE W1700
 - Affected versions: All versions < V1.1
 - Remediation: Update to V1.1
 - Download: <https://support.siemens.com/cs/wm/view/109762253>
- * SCALANCE W700
 - Affected versions: All versions < V6.4
 - Remediation: Update to V6.4 or any later version
 - Download: <https://support.siemens.com/cs/wm/view/109773308>

Machine-readable?

following specific workarounds and mitigations that mitigate the risk:

-CCMP instead of TKIP in the WPA/WPA2 protocol for both SCALANCE W-700 and W-1700 Management (web server). For more information, see the User Manual.

IONS

Siemens strongly recommends to protect the IT environment. In order to protect the IT environment, Siemens recommends to follow the operational guidelines provided in the operational-guidelines-industrial-security, sections in the product manuals.

Justin Murphy
April 12, 2024

What if there is no advisory?

Search for a press statement

Look into license documents

Check the SBOM

Use a vulnerability scanner

Contact the vendor!



Justin Murphy
April 12, 2024

Problems we're facing

Many vendors – all with different formats and distribution methods

Number of CVEs and security advisories is rising

SBOM adds to overload

Not every vulnerability can be exploited



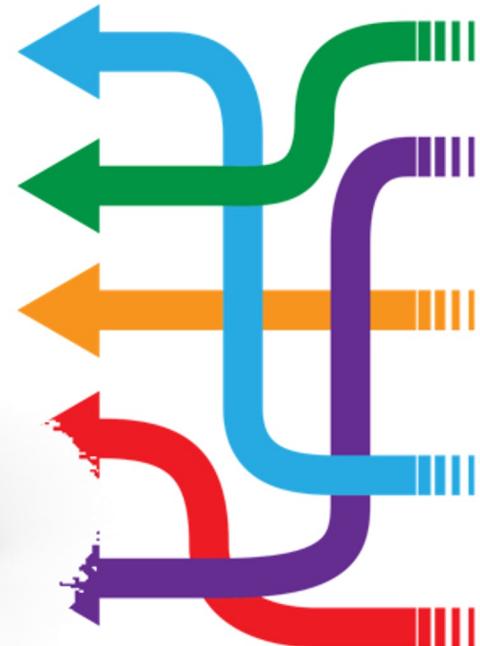
Scalability



Exploitability



What do we do?



Justin Murphy
April 12, 2024

Common Security Advisory Framework (CSAF)

International, open and free OASIS standard

Machine-readable format for security advisories (JSON) and VEX

Standardized way for distribution of security advisories

Build with automation in mind

Standardized tool set

Guidance to actionable information

Successor of CSAF CVRF 1.2



Ready to use!



Justin Murphy
April 12, 2024

Automated Process



Justin Murphy
April 12, 2024



Justin Murphy
April 12, 2024

CSAF Roles

<ul style="list-style-type: none">✓ Valid CSAF documents✓ File name restrictions✓ TLS enforced✓ TLP:WHITE freely accessible	CSAF publisher
<ul style="list-style-type: none">✓ Well-defined URL / security.txt / DNS => provider-<u>metadata.json</u>✓ List of advisories and latest changes and Fixed folder structure✓ or ROLIE feeds✓ Restriction on >=TLP:AMBER✓ All requirements from CSAF publisher	CSAF provider
<ul style="list-style-type: none">✓ Sign own advisories✓ Hash advisories✓ Published <u>OpenPGP</u> keys for integrity checks✓ All requirements from CSAF provider	CSAF trusted provider



Justin Murphy
April 12, 2024



Justin Murphy
April 12, 2024

What is VEX?

Vulnerability Exploitability eXchange (VEX) indicates the status of a software product or component with respect to a vulnerability.



Justin Murphy
April 12, 2024

What is VEX?

A common VEX use case is to indicate that software is or is not affected by a vulnerability.

Born from SBOM

Works with SBOM, or independently

Convey vulnerability status in a more standard way

One vulnerability, one status, one or more components

Machine readable



Status

Not affected

No remediation or mitigation is required. The vulnerability does not affect the listed products.

Affected

Actions are recommended to remediate, mitigate, or otherwise address the vulnerability. The vulnerability affects the listed products.

Fixed

The listed products contain fixes for the vulnerability.

Under investigation

The author of the VEX statement or other relevant parties are investigating and have not yet declared a final status.



Justin Murphy
April 12, 2024

“Not affected” justifications

Component not present

The vulnerable subcomponent is not included in the product.

Vulnerable code not present

The vulnerable subcomponent is included in the product but the vulnerable code is not present.

Vulnerable code not in execute path

The vulnerable code (likely in the subcomponent) cannot be executed due to the way it is used by the product.

Vulnerable code cannot be controlled by adversary

The vulnerable code is present and used by the product but cannot be controlled by an attacker to exploit the vulnerability.

Inline mitigations already exist

The product includes built-in protections or features that prevent exploitation of the vulnerability. These built-in protections cannot be subverted by the attacker and cannot be configured or disabled by the user. These mitigations completely prevent exploitation based on known attack vectors.



Justin Murphy
April 12, 2024

VEX Implementations

CSAF 2.0

Profile 5: VEX

CycloneDX

SPDX 3.0

OpenVEX



Justin Murphy
April 12, 2024

VEX publications

Vulnerability-Exploitability eXchange (VEX) – An Overview

September 2021

Vulnerability Exploitability eXchange (VEX) – Use Cases

April 2022

Vulnerability Exploitability eXchange (VEX) – Status Justifications

June 2022

Minimum Requirements for Vulnerability Exploitability eXchange (VEX)

April 2023

When to Issue VEX Information

November 2023



<https://www.cisa.gov/sbom>

Justin Murphy
April 12, 2024

Why VEX?

Allows for more efficient, prioritized, and automated vulnerability management

- Media-hyped vulnerabilities

- Reduce false positives

- Vendor-unaware customers

- Save money & reduce human workload!

Don't need an SBOM to VEX

Machine-readable allowing technology consumers, vendors, providers, and coordinators to accelerate vulnerability management.



Justin Murphy
April 12, 2024



Justin Murphy
April 12, 2024

CISA: VM & Supply Chain Transparency/Security



Justin Murphy
April 12, 2024



BLOG

Transforming the Vulnerability Management Landscape

Released: November 10, 2022

Revised: November 14, 2022

Eric Goldstein, Executive Assistant Director for Cybersecurity



In the current risk environment, organizations of all sizes are challenged to manage the number and complexity of new vulnerabilities. Organizations with mature vulnerability management programs seek more efficient ways to triage and prioritize efforts. Smaller organizations struggle with understanding where to start and how to allocate limited resources. Fortunately, there is a path toward more efficient, automated, prioritized vulnerability management. Working with our partners across government and the private sector, we are excited to outline three critical steps to advance the vulnerability management ecosystem:

- First, we must introduce greater automation into vulnerability management, including by expanding use of the Common Security Advisory Framework (CSAF)
- Second, we must make it easier for organizations to understand whether a given product is impacted by a vulnerability through widespread adoption of Vulnerability Exploitability eXchange (VEX)





BLOG

Transforming Vulnerability Management: CISA Adds OASIS CSAF 2.0 Standard to ICS Advisories

Released: September 29, 2023

By Lindsey Cerkovnik, Chief of Vulnerability Response and Coordination, and Daniel Larson, Justin Murphy, and Brandon Tarr

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [CYBER THREATS AND ADVISORIES](#)



In our pursuit to "[transform the vulnerability management landscape](#)," CISA is excited to announce that our security advisories for **Industrial Control Systems (ICS)**, **Operational Technology (OT)**, and Medical Devices now include the OASIS Common Security Advisory Framework (CSAF) Version 2.0 standard.

In the current risk environment, organizations are challenged to manage the growing number and complexity of new vulnerabilities. A critical step in helping organizations achieve better efficiency in triaging and prioritizing



Organization publishing CSAF



ORACLE

SICK

Sensor Intelligence.

Schneider
Electric

 **Hitachi Energy**



IBM



Federal Office
for Information Security



National Cyber Security Centre
Ministry of Justice and Security

NCSC-NL

SIEMENS

TIBCO™



Red Hat

FESTO

ARISTA

Justin Murphy
April 12, 2024

Where to find more information? <https://csaf.io>

OASIS TC: CSAF website: https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=csaf

CSAF GitHub: <https://github.com/oasis-tcs/csaf>

CSAF 2.0 JSON Schema: https://docs.oasis-open.org/csaf/csaf/v2.0/csaf_json_schema.json

CSAF 2.0 Prose: <https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html>

CSAF 2.0 Examples: https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples

CSAF author guide: <https://secvisogram.github.io/secvisogram-documentation/>

Secvisogram online editor: <https://secvisogram.github.io>



Justin Murphy
April 12, 2024

Tools developed by community

- CSAF producer: <https://github.com/secvisogram/secvisogram> or <https://github.com/mfd2007/yace>
- CSAF content management system: <https://github.com/secvisogram/secvisogram> + <https://github.com/secvisogram/csaf-cms-backend> (*WIP*)
- CSAF trusted provider: https://github.com/csaf-poc/csaf_distribution
- CSAF aggregator: https://github.com/csaf-poc/csaf_distribution (*WIP*)
- Provider checker: https://github.com/csaf-poc/csaf_distribution (*WIP*)
- CSAF downloader: https://github.com/csaf-poc/csaf_distribution
- CSAF full validator: <https://github.com/secvisogram/csaf-validator-service>



Justin Murphy
April 12, 2024

Future of CSAF

v2.1 in development

Incorporating other updated standards

CVSS 4.0

TLP 2.0

Clarifying updates

Several enhancements to the schema.

Future-proofing the standard?



<https://github.com/oasis-tcs/csaf/issues?q=is%3Aissue+is%3Aopen+label%3A%22csaf+2.1%22>



Justin Murphy
April 12, 2024

Future of CSAF @ CISA

Adoption

Improve tooling

Implementation guidance

CVD Team encourage/incentivize vendors to provide advisories in CSAF

Customers need to ask for them

More trainings & workshops (May 13-17 in Germany)

CSAF Aggregator

Work to improve data quality throughout ecosystem



Justin Murphy
April 12, 2024

What's next for SBOM/VEX?

Update to Minimum Requirements

SBOM+VEX part of a “balanced breakfast”

CISA continues to promote machine-readability for vulnerability data

Working with federal partners/regulators to understand dynamic landscape of vulns

Hybrid SBOM-a-rama in September in Denver, CO

CISA SBOM Working group(s)

Consolidating to one weekly meeting (April 15)



Justin Murphy
April 12, 2024

Call to Action and Questions?

Please join the conversation and/or contribute:

<https://github.com/oasis-tcs/csaf>

<https://github.com/oasis-tcs/openeox>

Contact: justin.murphy@cisa.dhs.gov

For information and questions about VEX and SBOM:

Contact: SBOM@cisa.dhs.gov

Questions?



Justin Murphy
April 12, 2024