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

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

Log4Shell™

Justin Murphy
April 12, 2024

Manual Process

1

Vendors

Produce and publish human-readable advisories.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Prioritizes the vulnerabilities based on criticality.

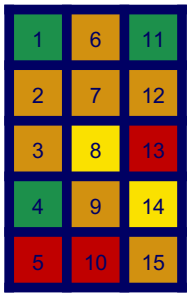
4

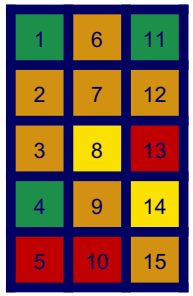
Customer

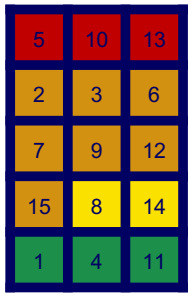
Affected products? Does risk assessment. Decides actions.

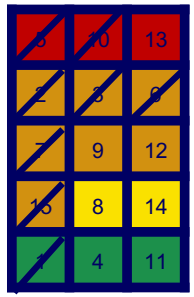
Severity

- critical
- high
- mediu m
- low









Justin Murphy
April 12, 2024

Manual Process

1

Vendor

Produces and publishes a human-readable advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Prioritizes the vulnerabilities based on criticality.

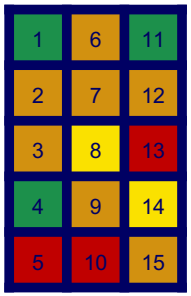
4

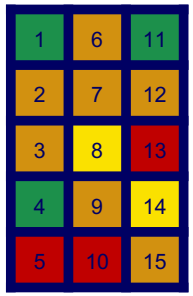
Customer

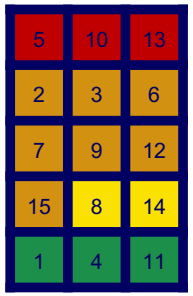
Affected products? Does risk assessment. Decides actions.

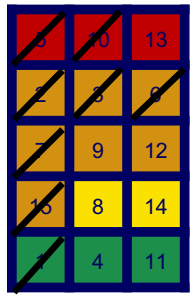
Severity

- critical
- high
- mediu m
- low

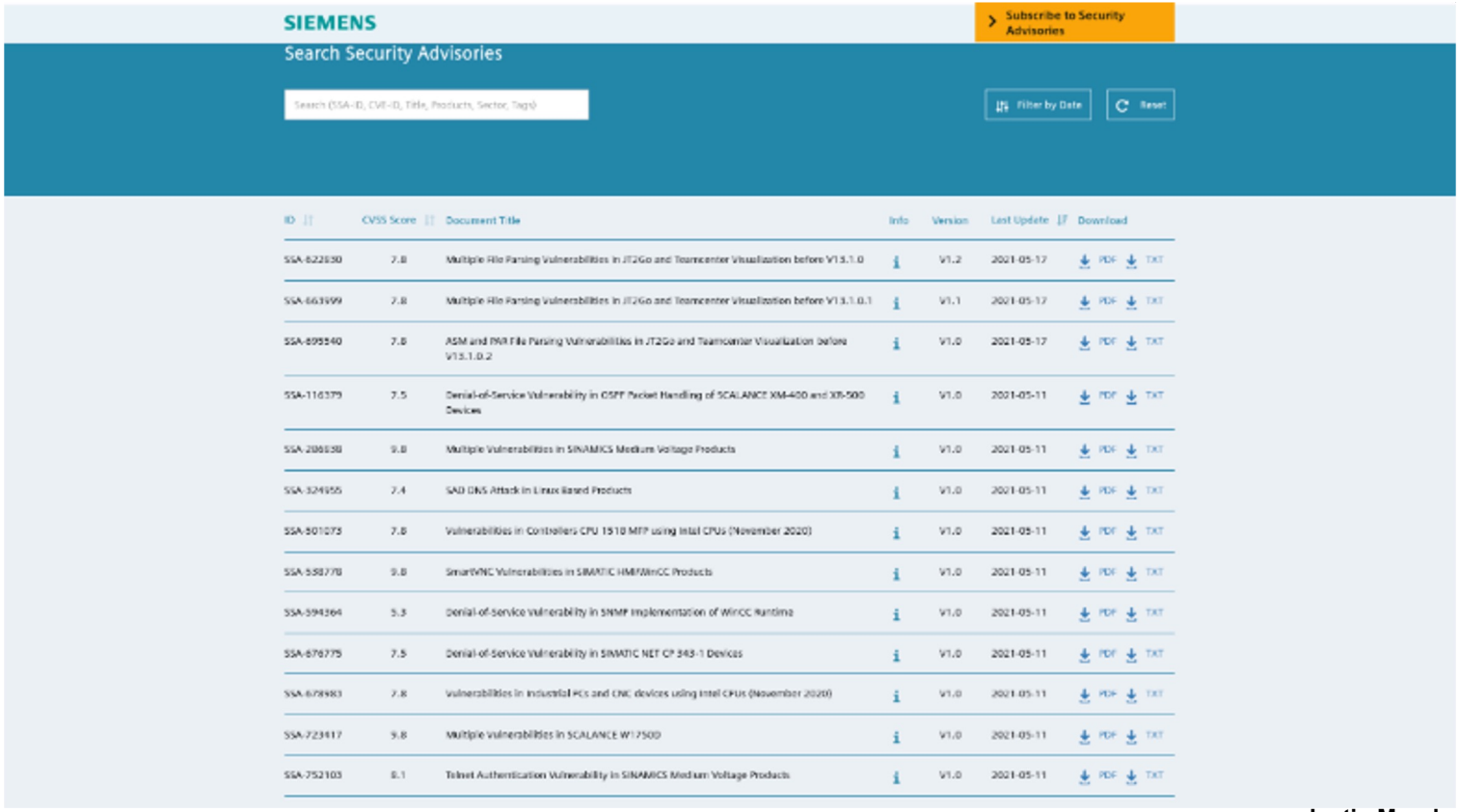




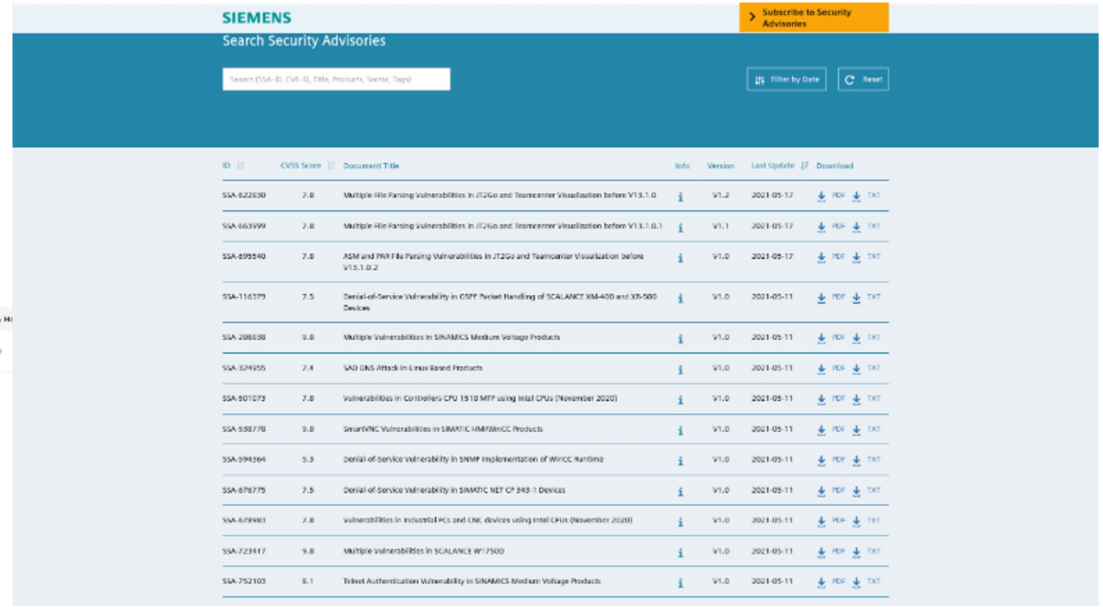


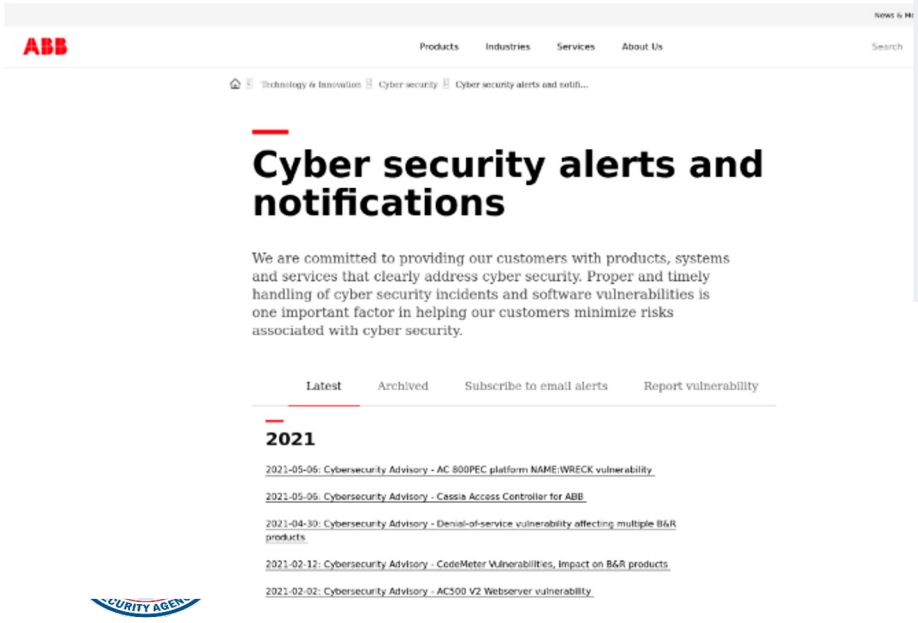


Justin Murphy
April 12, 2024

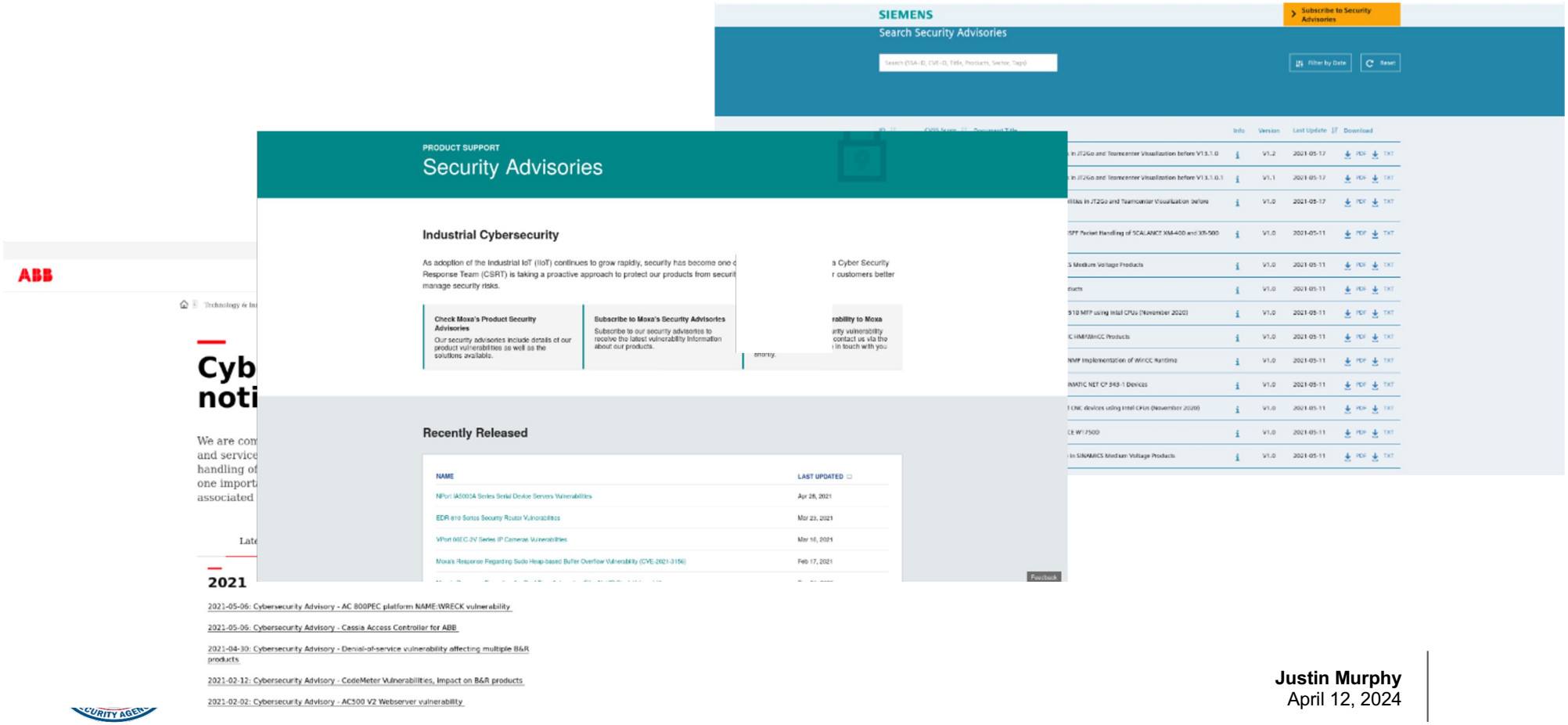


Justin Murphy
April 12, 2024

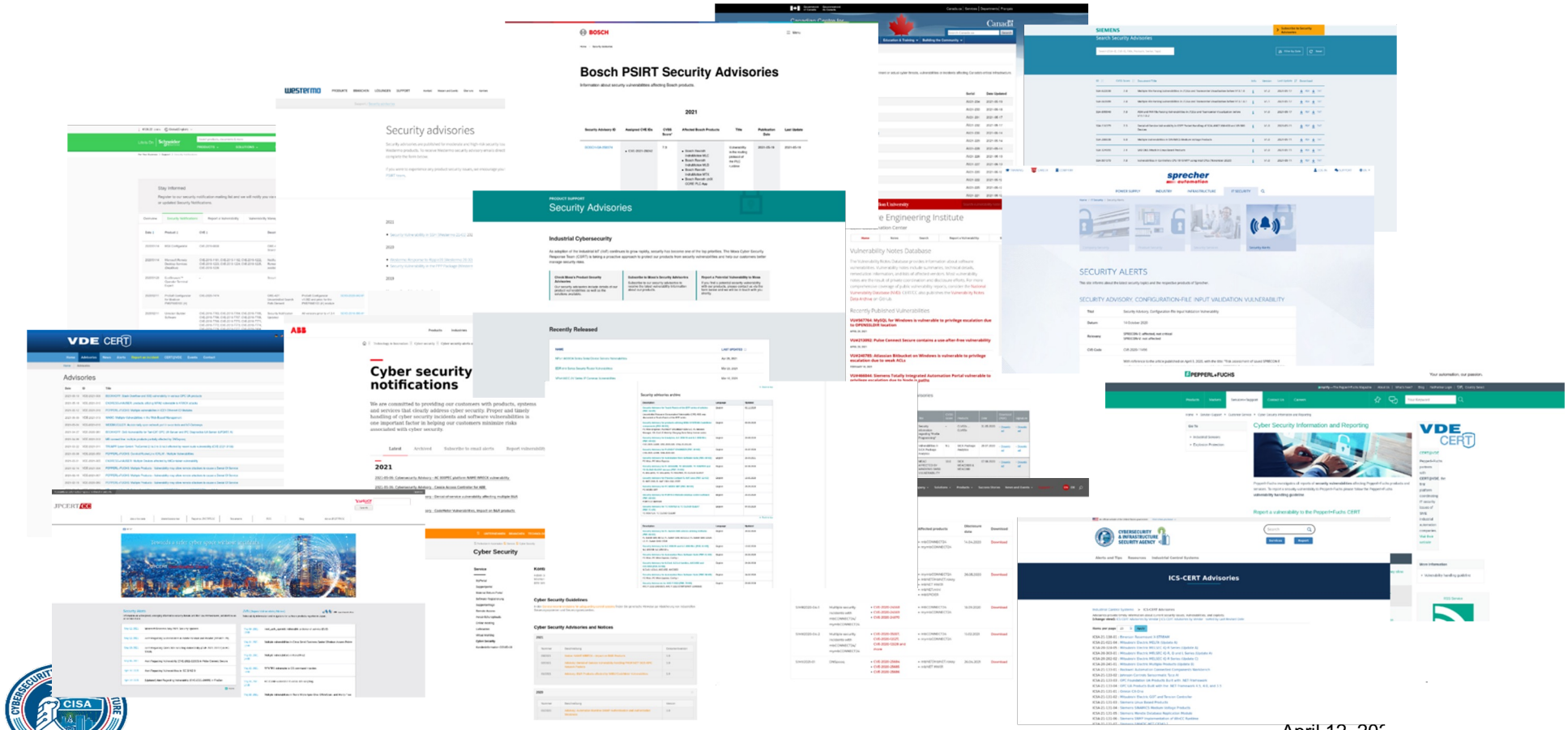




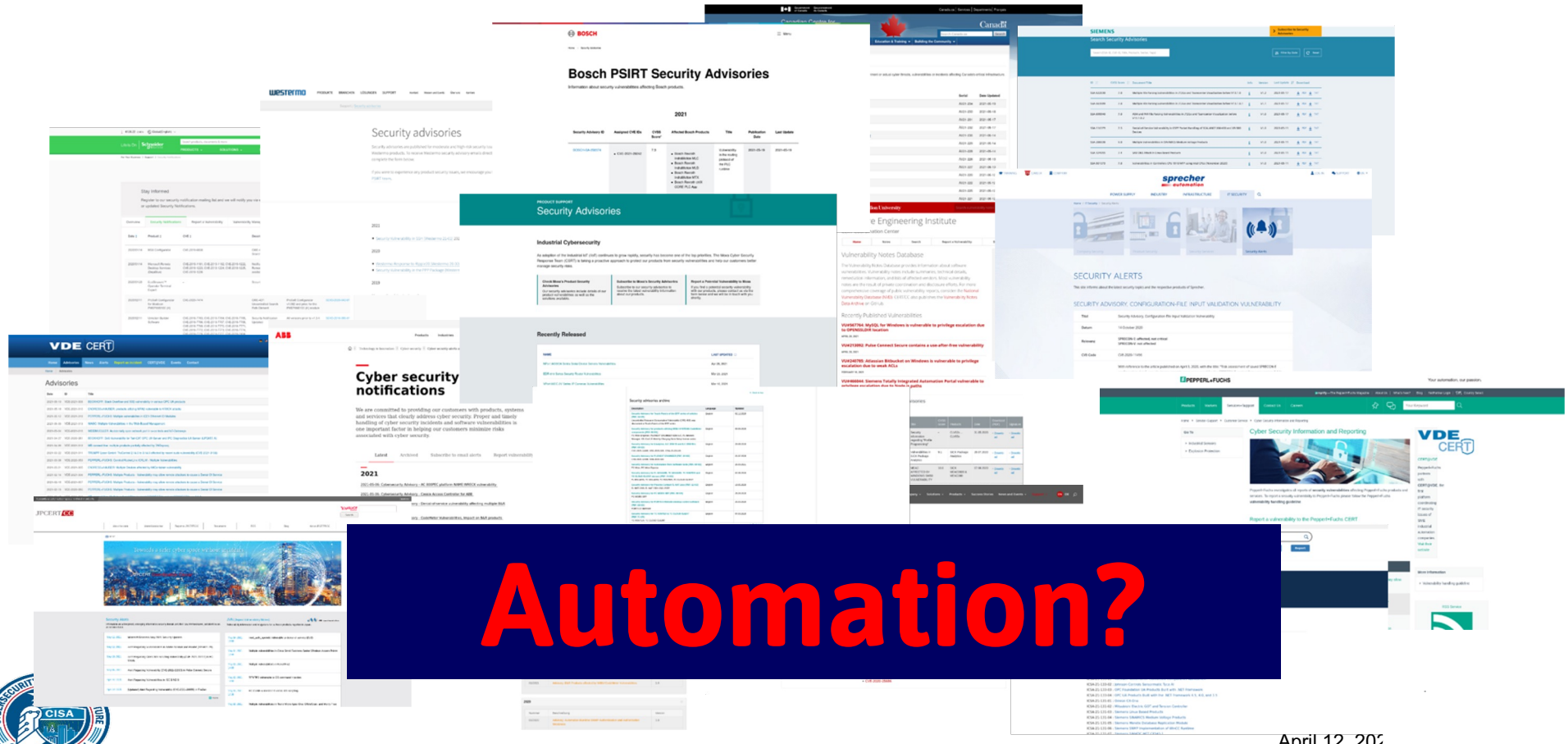
Justin Murphy
April 12, 2024



Justin Murphy
April 12, 2024


Bosch PSIRT Security Advisories
Security advisories
Security Advisories
Industrial Cybersecurity
Recently Released
VDE CERT
Advisories
Cyber security notifications
Cyber Security
Cyber Security Guidelines
Cyber Security Advisories and Notices
SECURITY ALERTS
Cyber Security Information and Reporting
ICS-CERT Advisories

April 12, 202


Bosch PSIRT Security Advisories
Security advisories
Security Advisories
Industrial Cybersecurity
Recently Released
Cyber security notifications
SECURITY ALERTS
Automation?

April 12, 202

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

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

Services

Alerts and Tips Resources Industrial Control Systems

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

ICS Advisory (ICSA-21-138-01)

More ICS-CER

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 th 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 Sensit 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

Life Is On Schneider Electric

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 SCADA solutions.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

Affected Products and Versions

- ClearSCADA, all versions
- EcoStruxure Geo SCADA Expert 2019, all versions
- EcoStruxure Geo SCADA Expert 2020, V83.7742.1 and prior

Vulnerability Details

CVE ID: **CVE-2021-22741**

CVSS v3.1 Base Score 6.7 | Medium | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-916: Use of Password Hash with Insufficient Computational Effort* vulnerability exists that could cause the revealing of account credentials 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:

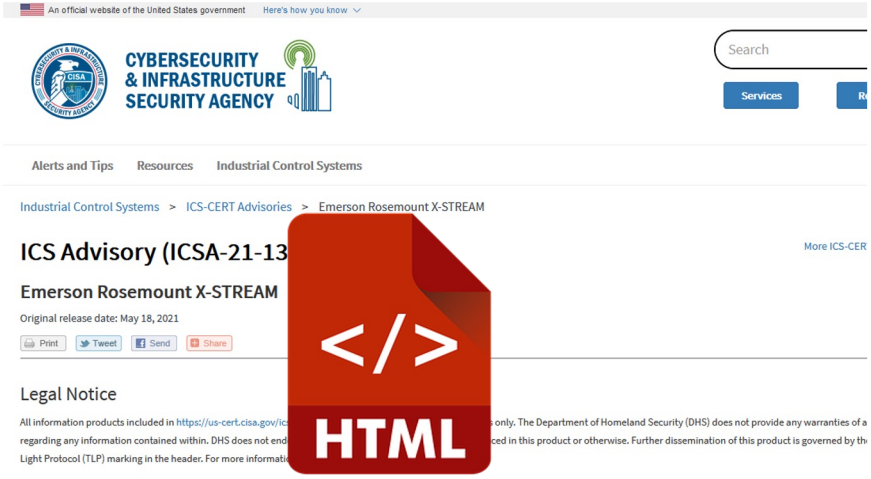
https://tprojects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads

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:   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 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/ww/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/ww/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



1. EXECUTIVE SUMMARY

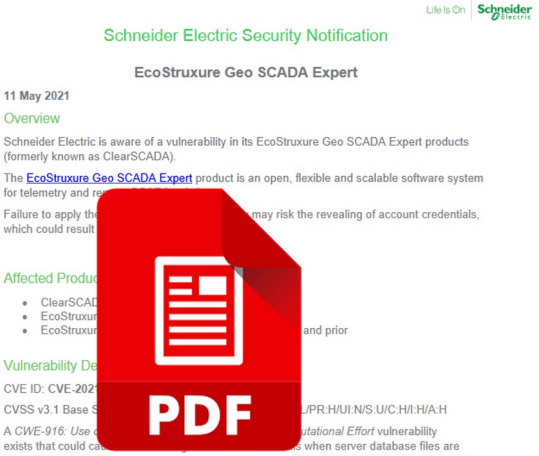
- CVSS v3 7.5
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing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

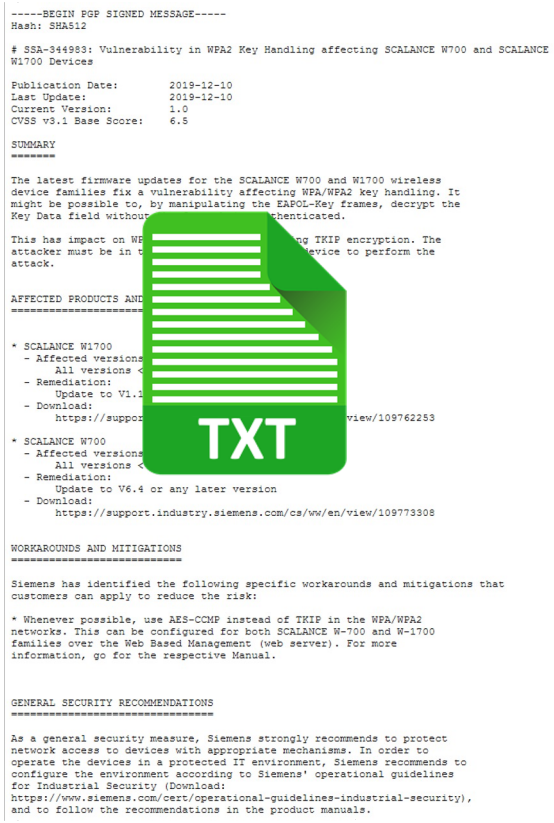
2. RISK EVALUATION

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

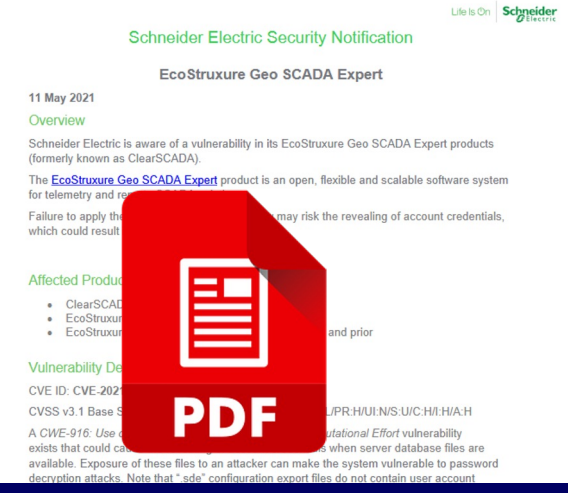
3. TECHNICAL DETAILS

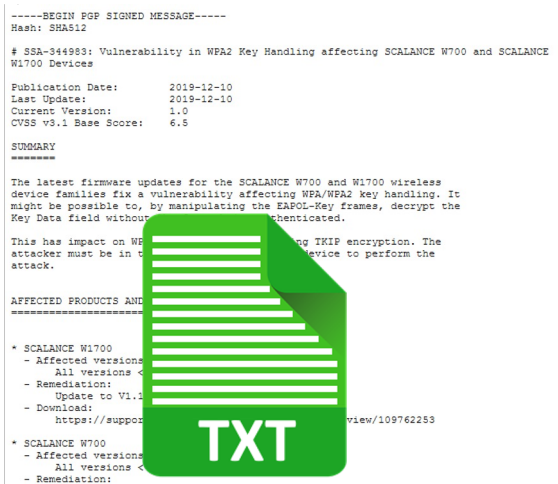
3.1 AFFECTED PRODUCTS





Justin Murphy
April 12, 2024





Machine-readable?

ustin 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!

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

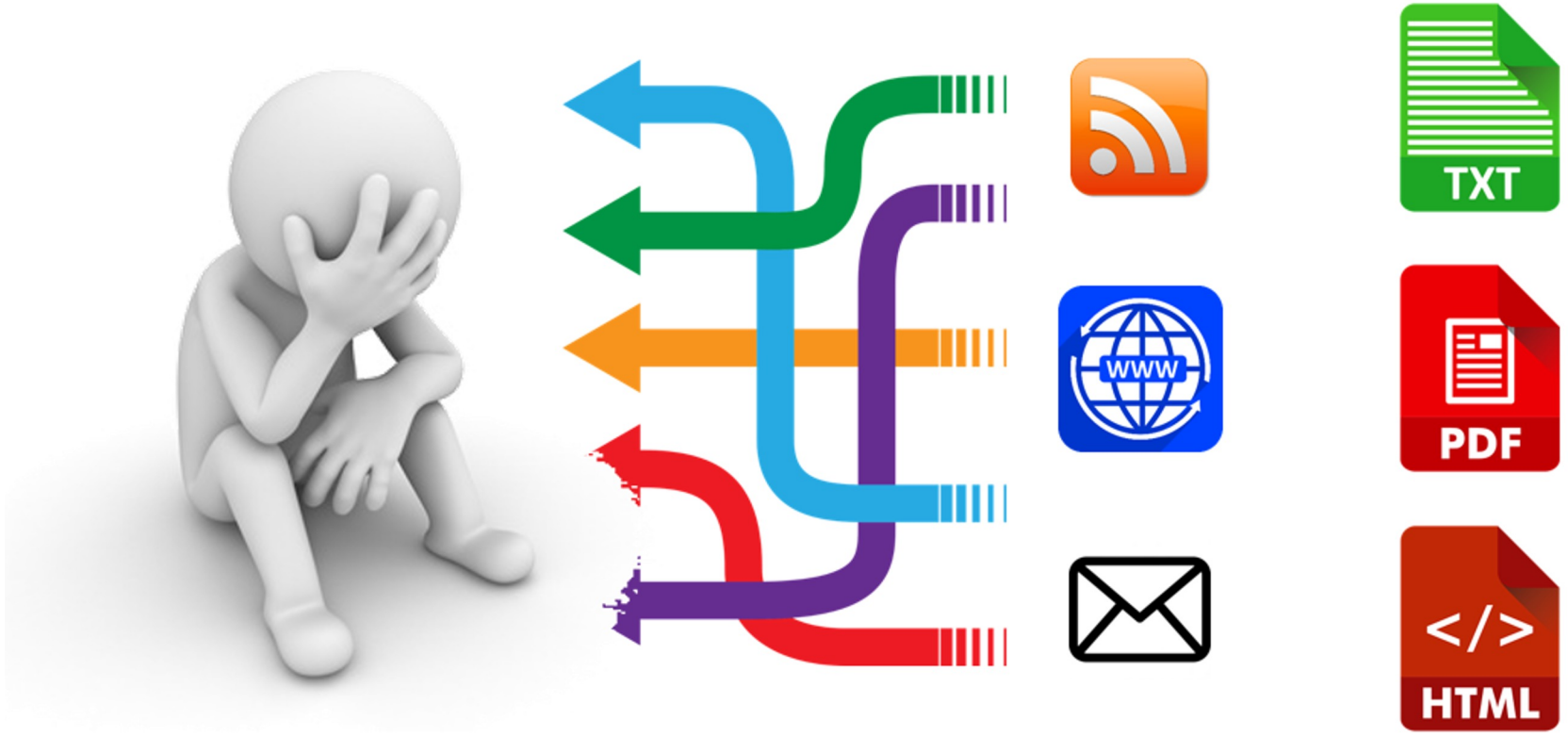
Scalability

Not every vulnerability can be exploited

Exploitability

Justin Murphy
April 12, 2024

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

Automated

Automated

1

Vendor

Produces and publishes **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Affected products? Risk Assessment (static)=>adopt criticality

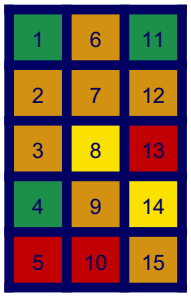
4

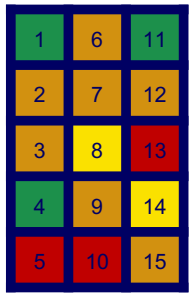
Customer

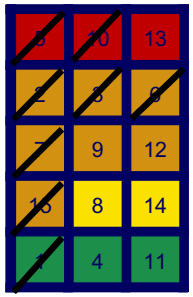
Sort advisories with affected products by criticality. Decide actions.

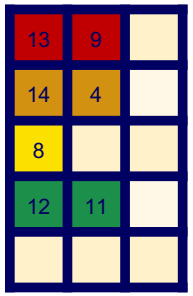
Severity

- critical
- high
- mediu m
- low









Justin Murphy
April 12, 2024

CSAF

Justin Murphy
April 12, 2024

CSAF Roles

✓ Valid CSAF documents ✓ File name restrictions ✓ TLS enforced ✓ TLP:WHITE freely accessible	CSAF publisher
✓ Well-defined URL / security.txt / DNS => provider-metadata.json ✓ List of advisories and latest changes and Fixed folder structure ✓ or ROLIE feeds ✓ Restriction on >=TLP:AMBER ✓ All requirements from CSAF publisher	CSAF provider
✓ Sign own advisories ✓ Hash advisories ✓ Published OpenPGP 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.

“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.

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

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

CSAF

+VEX

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

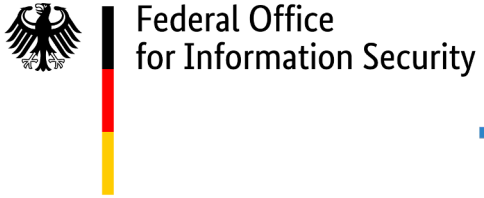
By Lindsey Cerkovnik, Chief of Vulnerability Response and Coordination, and Daniel Larson, Justin Murphy, and Brandon Tarr

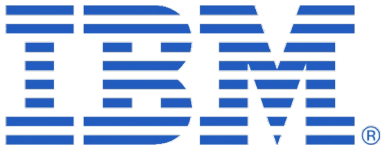
RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CYBER THREATS AND ADVISORIES

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





NCSC-NL

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

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)

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?