Vulnerability management with CSAF – why SBOM is not enough

Thomas Schmidt
Federal Office for Information Security (BSI)
Who am I?

**Thomas Schmidt**

Technical ICS Analyst @BSI
(usually not into standardization)

First day at work: analyze TRITON / TRISIS
Passion for
- ICS
- International Cooperation
- CVD
- Capacity building
Vulnerability management

- Know the vulnerability
  - Details
  - Impact
  - Risks
  - Exploitability
  - ...

- Know where the component is used

- Know how to remediate
  - What do I need to do?
Vulnerability management

• Know the vulnerability
  • Details
  • Impact
  • Risks
  • Exploitability
  • ...

• Know where the component is used

• Know how to remediate
  • What do I need to do?

CVE
SBOM
Security Advisory

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Just knowing the component is included is not enough...
Just knowing the component is included is not enough...

... as you usually don’t have them in your asset database
Just knowing the component is included is not enough...

...as it says nothing whether the vulnerability is exploitable in the product

With these advances, described further below, we will make necessary progress in vulnerability management and reduce the window that our adversaries have to exploit American networks.


When a new vulnerability is identified, software vendors jump into action: understanding impacts to products, identifying remediations, and communicating to end users. But as we know, the clock is ticking: adversaries are often turning vulnerabilities to exploits within hours of initial public reports.

Software vendors work constantly to understand if their products are impacted by a new vulnerability. To meet this timeframe, our community needs a standardized approach for vendors to disclose security vulnerabilities to end users in an accelerated and automated way.

The CSAF, developed by the OASIS CSAF Technical Committee, is a standard for machine-readable security advisories. CSAF provides a standardized format for ingesting vulnerability advisory information and simplify triage and remediation processes for asset owners. By publishing security advisories using CSAF, vendors will dramatically reduce the time required for enterprises to understand organizational impact and drive timely remediation.

2. Clarifying Impact: Use Vulnerability Exploitability eXchange (VEX) to communicate whether a product is affected by a vulnerability and enable prioritized vulnerability response

https://www.cisa.gov/blog/2022/11/10/transforming-vulnerability-management-landscape
Security Advisories

- Details about the vulnerabilities (including a CVE)
- **Products that are affected**
- Remediation
- Scores
- General guidance
CVE vs. Advisories

CVE

One vulnerability

Focus: Talk about the same thing

Advisory

One or multiple vulnerabilities

Focus: Tell remediation
Security Advisories

- Details about the vulnerabilities (including a CVE)
- Products that are affected
- **Remediation**
- Scores
- General guidance
Security Advisories

• Details about the vulnerabilities (including a CVE)
• Products that are affected
• **Remediation**
  • Hotfix
  • Update
  • Upgrade
  • *Mitigating countermeasures*
  • ...
• Scores
• General guidance

Patch
For each new vulnerability, decide

- Patch immediately
- Patch next downtime
- Accept risk
How to decide?
Risk and cost scales depend on:
- Vulnerability
- Safety impact
- Usage of the product
- Existing countermeasures in the infrastructure
- Likelihood of broken patches / incompatibilities
- Attacks in the wild
Where do I get the information?
Security advisories!
Some examples
Manual process

- Production of human-readable advisory
- Publication

Severity of advisory
- low
- medium
- high
- critical

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

Vendor
- Production of human-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Severity of advisory
critical
green
medium
yellow
high
orange
low
red

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

**Vendor**
- Production of human-readable advisory
- Publication

**Find**
- Search websites for new / updated advisories
- Download

**Prioritize**
- Sift criticality of vulnerabilities

Severity of advisory:
- Low
- Medium
- High
- Critical
Manual process

Vendor
- Production of human-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Prioritize
- Sift criticality of vulnerabilities

Evaluate
- Do you have affected products?
- Risk assessment
- Decision which actions should be taken

Severity of advisory
- low
- medium
- high
- critical
Manual process

Vendor
- Production of human-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Prioritize
- Sift criticality of vulnerabilities

Evaluate
- Do you have affected products?
- Risk assessment
- Decision which actions should be taken

Severity of advisory
- low
- medium
- high
- critical

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Find

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

VDE CERT

Cyber security notifications

Cyber Security

Recently Published

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

VDE CERT

Cyber security notifications

Cyber Security

Recently Published

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

VDE CERT

Cyber security notifications

Cyber Security

Recently Published

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

VDE CERT

Cyber security notifications

Cyber Security

Recently Published

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

VDE CERT

Cyber security notifications

Cyber Security

Recently Published

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

VDE CERT

Cyber security notifications

Cyber Security

Recently Published

Bosch PSIRT Security Advisories

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Analyze

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt

ICS Advisory (ICSA-21-138-01)

1. EXECUTIVE SUMMARY

- CVSS v3.1: 7.5
- CVSS v3.0: 7.5
- CVSS v2.0: 8.5
- Base Score: 7.5
- Impact Score: 1.4

2. RISK EVALUATION

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

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

- Emerson Rosemount X-STREAM Analysers
- Emerson Rosemount 5-STRAIN Gas Analyser

Legal Notice

The information provided below is for educational purposes only. The Rosemount Security Division cannot provide any warranties of any kind regarding the information contained within. This does not constitute any commitment or obligation from the part of Emerson Process Management, Inc. or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the headers. For more information about TLP, visit:

- https://www.emersonprocessmanagement.com/traffic-light-protocol

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 ClearSCADA Geo/SCADA Expert product is an open, flexible and scalable software system for balancing and remote SCADA solutions.

Failure to apply the corrections provided below may result in the revealing of account credentials, which could result in unauthorised system access.

Affected Products and Editions

- ClearSCADA, v11.0.0.29.234
- ClearSCADA, v11.0.0.29.278

Security Details

Version: 11.0.0.29.234

CVE-2020-8552

A Code Execution vulnerability in the EcoStruxure Geo SCADA Expert product could allow privilege escalation in certain circumstances. This vulnerability exists in the following versions:

- ClearSCADA Geo/SCADA Expert v11.0.0.29.234

Remediation

Update to version 11.0.0.29.278.

- https://www.emersonprocessmanagement.com/downloads/patch-notes/clearscada-11.0.0.29.278
- https://www.emersonprocessmanagement.com/downloads/patch-notes/clearscada-11.0.0.29.234

Further information is available online at:

- https://www.emersonprocessmanagement.com/downloads/patch-notes/clearscada-11.0.0.29.278
Number of Advisories
Number of Advisories CVE

https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/
That doesn't scale!
Possible solutions
Let’s automate the process...
Process with CSAF

Vendor
- Production of *machine-readable* advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Evaluate (static)
- Do you have affected products?
- Risk assessment (static) => adopt criticality
- Criticality of the vulnerability

Measures
- Sift of advisories with affected products sort by criticality
- Decision which actions should be taken

Severity of advisory
- low
- medium
- high
- critical
What is CSAF?

**Common Security Advisory Framework**
- International, open and free standard
- Machine-readable format for security advisories (JSON)
- Standardized way of distribution security advisories
- Build with automation in mind
- Standardized tool set
- Guidance to actionable information
- Successor of CSAF CVRF 1.2

Ready to use!
Requirements for asset owners

• Machine-readable asset inventory
• Request Advisories in CSAF from vendors
• Connection between both of them to leverage the full potential
Vendors’ Perspective
Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

Vendor prepares patch

Vendor writes advisory

Vendor publishes advisory & patch

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

Vendor prepares patch

Vendor writes advisory

CSAF content management system

Vendor publishes advisory & patch

CSAF trusted provider
Coordinator (CVD)

- Coordinator becomes aware of a vulnerability
- Coordinator contacts vendor
- Coordinator runs CVD case
- Coordinator writes advisory
- CSAF content management system
- Coordinator publishes advisory
- CSAF trusted provider
Distribution
**Where to find CSAF documents?**

<table>
<thead>
<tr>
<th>Valid CSAF documents</th>
<th>CSAF publisher</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name restrictions</td>
<td></td>
</tr>
<tr>
<td>TLS enforced</td>
<td></td>
</tr>
<tr>
<td>TLP:WHITE freely accessible</td>
<td></td>
</tr>
</tbody>
</table>

| Well-defined URL / security.txt / DNS => provider-metada.json | CSAF provider |
| List of advisories and latest changes and Fixed folder structure |                |
| or ROLIE feeds |                |
| Restriction on >=TLP:AMBER |                |
| All requirements from CSAF publisher |                |

<table>
<thead>
<tr>
<th>Sign own advisories</th>
<th>CSAF trusted provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash advisories</td>
<td></td>
</tr>
<tr>
<td>Published OpenPGP keys for integrity checks</td>
<td></td>
</tr>
<tr>
<td>All requirements from CSAF provider</td>
<td></td>
</tr>
</tbody>
</table>

https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html#7-distributing-csaf-documents
Everything perfect?
Obviously not! Still many sources of information
One more step needed to make it easy … Saradi to the rescue!

CSAF aggregator
Scalable and resilient advisory distribution infrastructure (Saradi)

CSAF aggregator

- Trusted party
- Collects advisories from issuers
- Provides them
- API optional
- One-stop-shop
- Multiple around the world (National CERTs)
Users’ Perspective
User retrieves advisories

User compares with asset database

User decides what to do

User acts

User documents action
User retrieves advisories

Custom downloader

User compares with asset database

CSAF asset matching system

User decides what to do

SSVC

User acts

CSAF asset matching system

User documents action

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
User

User retrieves advisories

CSAF trusted provider

Custom downloader

User compares with asset database

CSAF asset matching system

SSVC

User decides what to do

User acts

User documents action

CSAF asset matching system

CSAF aggregator

CSAF provider

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Supply chain: vendors’ view
Supply chain

Vendor finds advisory of supplier

Vendor matches against own SBOMs

Vendor decides what to do

Vendor acts

Vendor publishes information

CSAF provider

CSAF trusted provider

CSAF aggregator

Custom downloader

CSAF SBOM matching system

SSVC

CSAF content management system

CSAF trusted provider

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Tools developed by the community

- CSAF producer: https://github.com/secvisogram/secvisogram
- CSAF trusted provider: https://github.com/csaf-poc/csaf_distribution
- CSAF aggregator: https://github.com/csaf-poc/csaf_distribution
- Provider checker: https://github.com/csaf-poc/csaf_distribution (WIP)
- CSAF management system: open for commercial and Open Source tools
- CSAF asset matching system: open for commercial and Open Source tools
- CSAF downloader: https://github.com/csaf-poc/csaf_distribution
- CSAF full validator: https://github.com/secvisogram/csaf-validator-service

- Your tools?
What about VEX?
• Vulnerability Exploitability eXchange
• Communicate product status explicit
  • Not affected
  • Affected
  • Fixed
  • Under investigation
• Machine-readable to address scalability
VEX and CSAF

- VEX is a profile in CSAF
- Specific, mandatory fields
- Uses same infrastructure and systems
- VEX is parallel to SBOM (not necessarily in the SBOM)
CSAF in Operation
Organizations publishing CSAF
Ecosystem

Vendor - Vendor - Vendor - Vendor

BSI CSAF trusted provider

CSAF Lister

https://wid.cert-bund.de

CSAF Aggregator

https://aggregator.cert-bund.de

User

Pull directly from source

Pull from aggregator

Collect list of potential sources

Pull

Manual Pull / Push

public

public

Pull

...
Conclusions
Two sides of the same coin – different maturity stages

Vendor

Vendor (specific) internal tools and processes

- Continuous Security Advisory Release (CSAR)
- Unique Product IDs
- Content Management System
- Text editor / Writer

Quality of advisories

- Supply Chain routinely included
- Input data for automatic asset management
- Existence of machine-readable format
- Existence of human-readable format

Asset owner

Asset owner (specific) internal tools and processes

- Routinely patching
- Automatic processing of advisories
- (Semi-) Automated processing of advisories
- Manual processing of advisories

Requirements for tools and processes

- Security downtime accepted/minimized/mitigated
- Asset management system with unique Product IDs
- Asset management with smart search
- Web browser

Two sides of the same coin – different maturity stages
Next step: reach stage 2 across parties

**Vendor**
- Vendor (specific) internal tools and processes
  - Continuous Security Advisory Release (CSAR)
  - Unique Product IDs
  - Content Management System
  - Text editor / Writer
- Quality of advisories
  - Supply Chain routinely included
  - Input data for automatic asset management
  - Existence of machine-readable format
  - Existence of human-readable format

**Asset owner**
- Asset owner (specific) internal tools and processes
  - Routinely patching
  - Automatic processing of advisories
  - (Semi-) Automated processing of advisories
  - Manual processing of advisories
- Requirements for tools and processes
  - Security downtime accepted/minimized/mitigated
  - Asset management system with unique Product IDs
  - Asset management with smart search
  - Web browser

**Difficulty**

Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt
Key takeaways & actions

- Number of vulnerabilities discovered is rising => number of advisories as well
- Advisories are needed for risk-based decisions
- Automation is possible – so automate the boring stuff

- Request your vendors to provide CSAF 2.0
- Provide CSAF documents to your customers to ease their pain
- Send out VEX as CSAF to use the same tools
- **Spread the word! #oCSAF #advisory**
Where to find more information?
https://csaf.io


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

Secvisogram sources: https://github.com/secvisogram/secvisogram
Running Demo: https://secvisogram.github.io