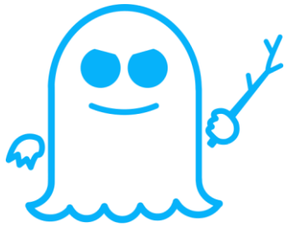
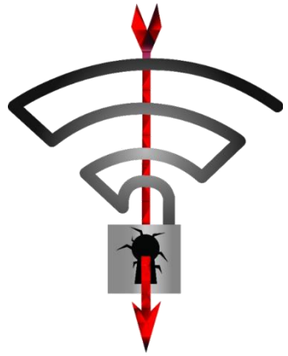
Your Software IS/NOT Vulnerable: CSAF, VEX and the Future of Advisories

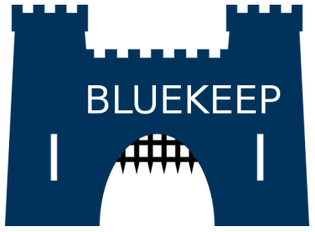
Allan Friedman & Thomas Schmidt

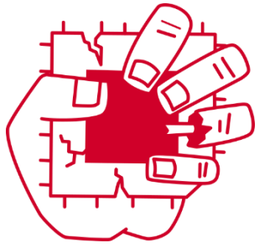
This talk is *not* about SBOM...



SPECTRE

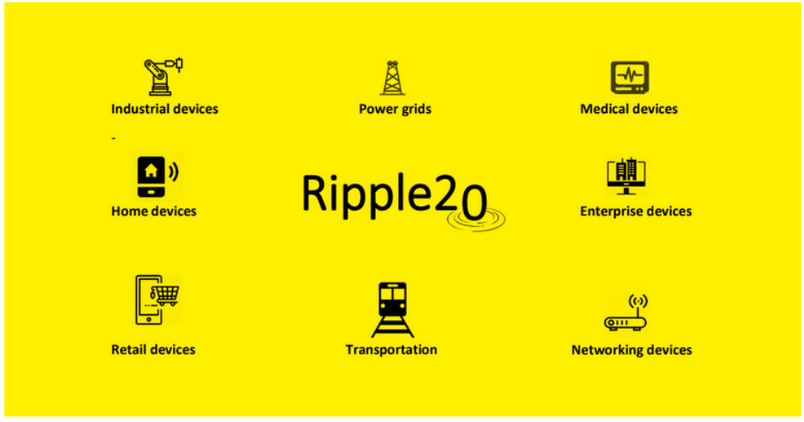






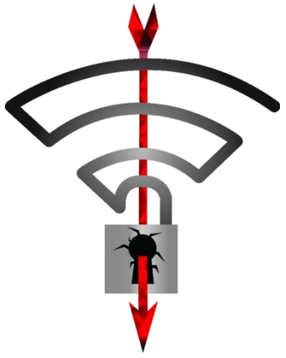
MELTDOWN

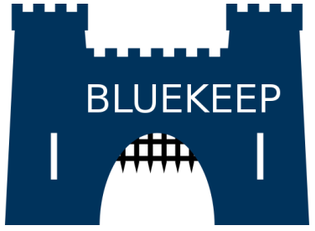
FORESHADOW

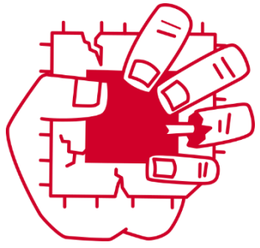


Known vulnerabilities
Should be the easiest part

SPECTRE

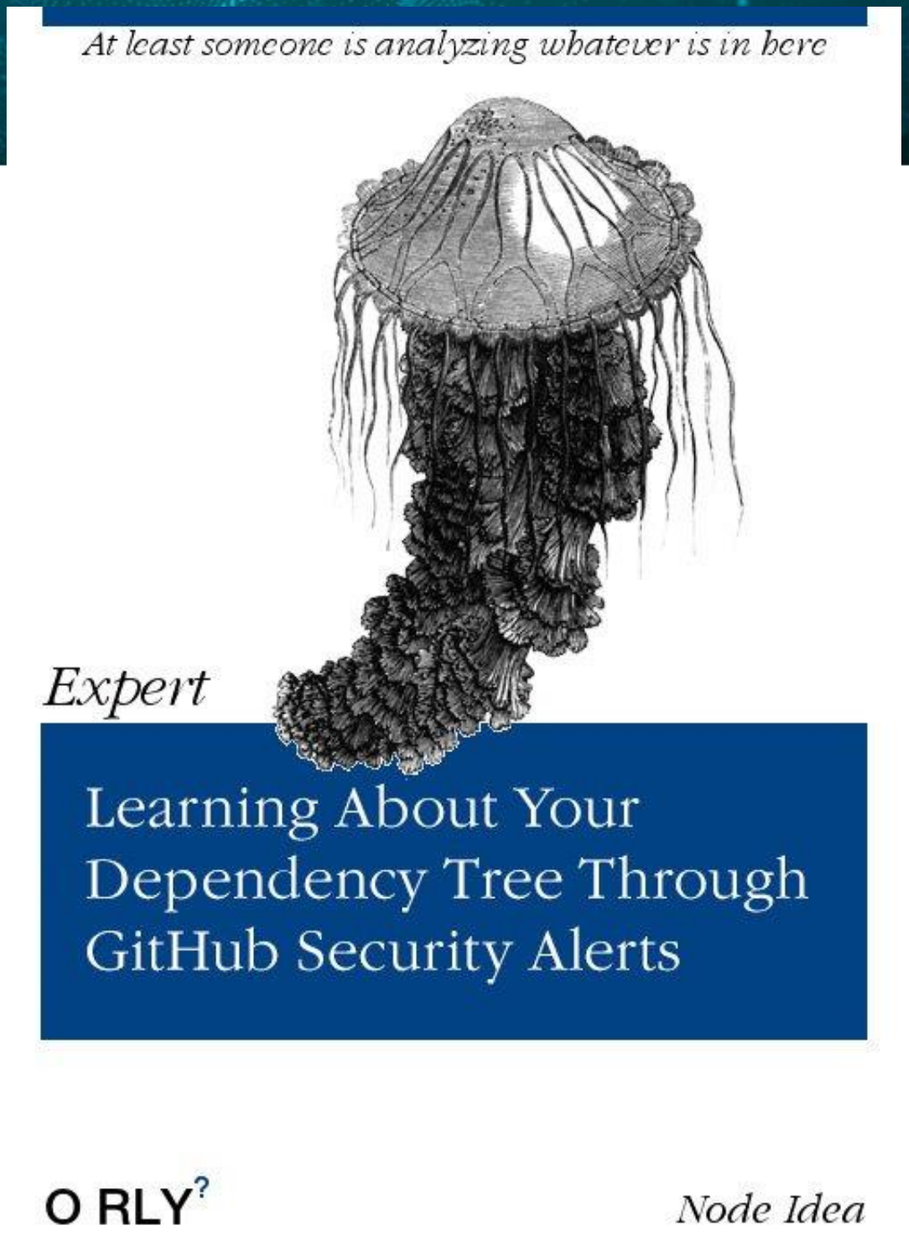






MELTDOWN

We will know about more potential vulnerabilities with SBOM



https://boyter.org/static/books/new2.jpg

How to communicate vulnerabilities?

CVE

How to communicate affected versions and remediations for vulnerabilities?

Security Advisories

Not all vulnerabilities are exploitable

We need a way to communicate that your product is not affected

Blog News Top News

Zephyr Security Update on Amnesia:33

December 16, 2020

Written by David Brown, on behalf of the Zephyr Security Team

On December 8, 2020, Forescout released a report containing numerous vulnerabilities found in various embedded TCP/IP stacks, known as AMNESIA:33. These vulnerabilities, across multiple network implementations, concern various memory and overflow errors, some of which are readily exploitable.

The Zephyr project received notification of this vulnerability through CERT before the publication date. We analyzed these vulnerabilities, and any affected code, and concluded that the **Zephyr project is not impacted by any of these vulnerabilities, neither in the current releases, nor in any Long Term Support release.**

Despite being collected under a single name, this report describes 33 vulnerabilities that are largely unrelated to one another. The report is the result of an analysis of 4 TCP/IP implementations that are commonly used in embedded systems: uIP, uIP in Contiki-OS, PicoTCP, and Fnet. Of these implementations, only the code in Fnet has ever been used in Zephyr.

The Zephyr LTS release 1.14 contains an implementation of the TCP stack from Fnet. Of the vulnerabilities reported in Fnet, 2, CVE-2020-17468, and CVE-2020-17469, are in the IPv6 Fnet code, one, CVE-2020-17467, affects Link-local Multicast Name Resolution LLMNR), and 2, CVE-2020-24383, and CVE-2020-17470 affect DNS functionality. None of the affected code has been used in the Zephyr project, while 1.14 does use the Fnet TCP, it does not use the affected IPv6, DNS or LLMNR code.

For current releases, including the current 2.4.0, this code has been replaced by a Zephyr-specific implementation.

The Zephyr project takes security seriously, for more information on our processes involving security, including how to report vulnerabilities can be found on our Security page.

Blog News Top News

Zephyr Security Update on Amnesia:33

December 16, 2020

Written by David Brown, on behalf of the Zephyr Security Team

The Zephyr project received notification of this vulnerability through CERT before the publication date. We analyzed these vulnerabilities, and any affected code, and concluded that the **Zephyr project is not impacted by any of these vulnerabilities, neither in the current releases, nor in any Long Term Support release.**

On December 8, 2020, Forescout released a report containing numerous vulnerabilities found in various embedded TCP/IP stacks, known as AMNESIA:33. These vulnerabilities, across multiple network implementations, concern various memory and overflow errors, some of which are readily exploitable.

The Zephyr project received notification of this vulnerability through CERT before the publication date. We analyzed these vulnerabilities, and any affected code, and concluded that the **Zephyr project is not impacted by any of these vulnerabilities, neither in the current releases, nor in any Long Term Support release.**

Despite being collected under a single name, this report describes 33 vulnerabilities that are largely unrelated to one another. The report is the result of an analysis of 4 TCP/IP implementations that are commonly used in embedded systems: uIP, uIP in Contiki-OS, PicoTCP, and Fnet. Of these implementations, only the code in Fnet has ever been used in Zephyr.

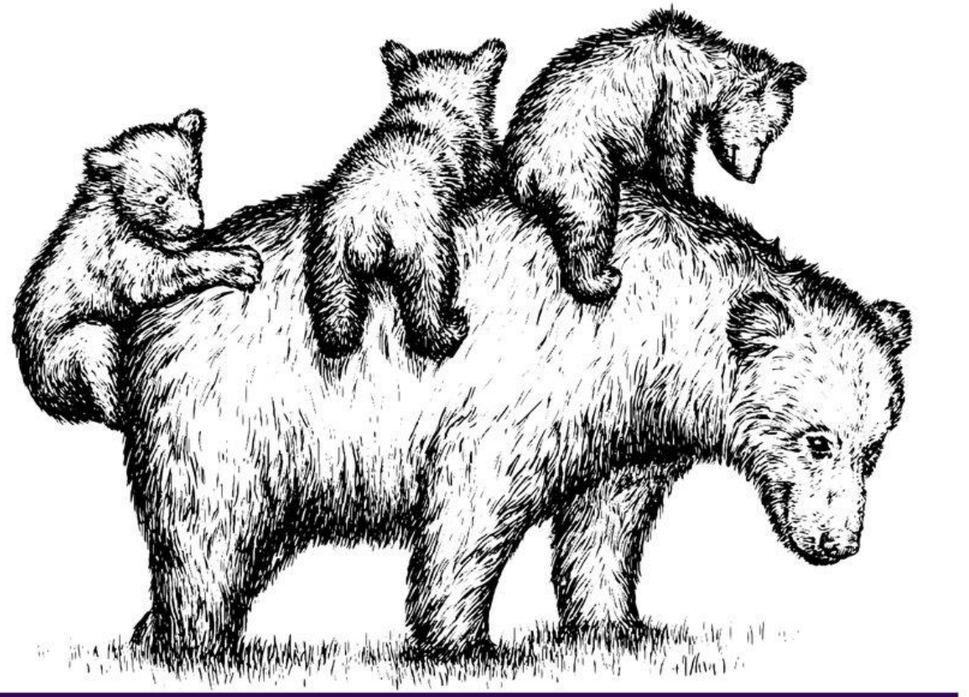
The Zephyr LTS release 1.14 contains an implementation of the TCP stack from Fnet. Of the vulnerabilities reported in Fnet, 2, CVE-2020-17468, and CVE-2020-17469, are in the IPv6 Fnet code, one, CVE-2020-17467, affects Link-local Multicast Name Resolution LLMNR), and 2, CVE-2020-24383, and CVE-2020-17470 affect DNS functionality. None of the affected code has been used in the Zephyr project, while 1.14 does use the Fnet TCP, it does not use the affected IPv6, DNS or LLMNR code.

For current releases, including the current 2.4.0, this code has been replaced by a Zephyr-specific implementation.

The Zephyr project takes security seriously, for more information on our processes involving security, including how to report vulnerabilities can be found on our Security page.

https://www.zephyrproject.org/zephyr-security-update-on-amnesia33/

Scaling



Getting the wrong idea from that conference talk you attended

Solving Imaginary Scaling Issues

At Scale

O RLY?

https://boyter.org/static/books/CxzX0scXUAA21uo.jpg

How many device types (Zephyr or other) are on your factory floor?

Does that method scale?

How to communicate that a device is (not) “exploitable”?

Vulnerability Exploitability eXchange (VEX)

“exploitable”

“affected”

Do I need to do anything?

“affected”

Actions are recommended to remediate or address this vulnerability.

This could include: learning more about the vulnerability and context, and/or making a risk-based decision to patch or apply defense-in-depth measures

“Not Affected”

You’re good.

“Not Affected”

No remediation is required regarding this vulnerability.

This could be because the code referenced in the vulnerability is not present, not exposed, compensating controls exist, or other factors.

What do we actually need for VEX

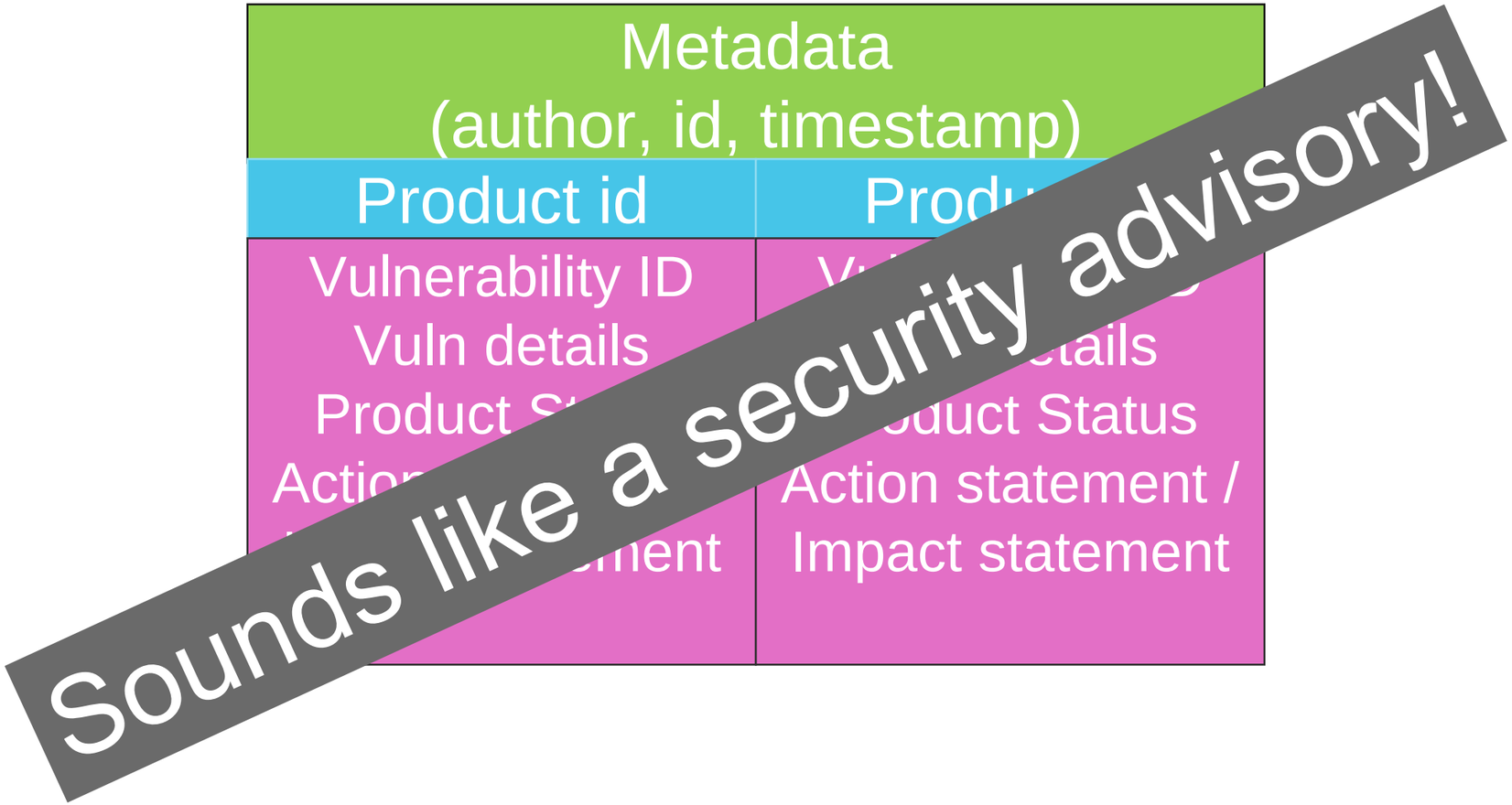
Machine readable

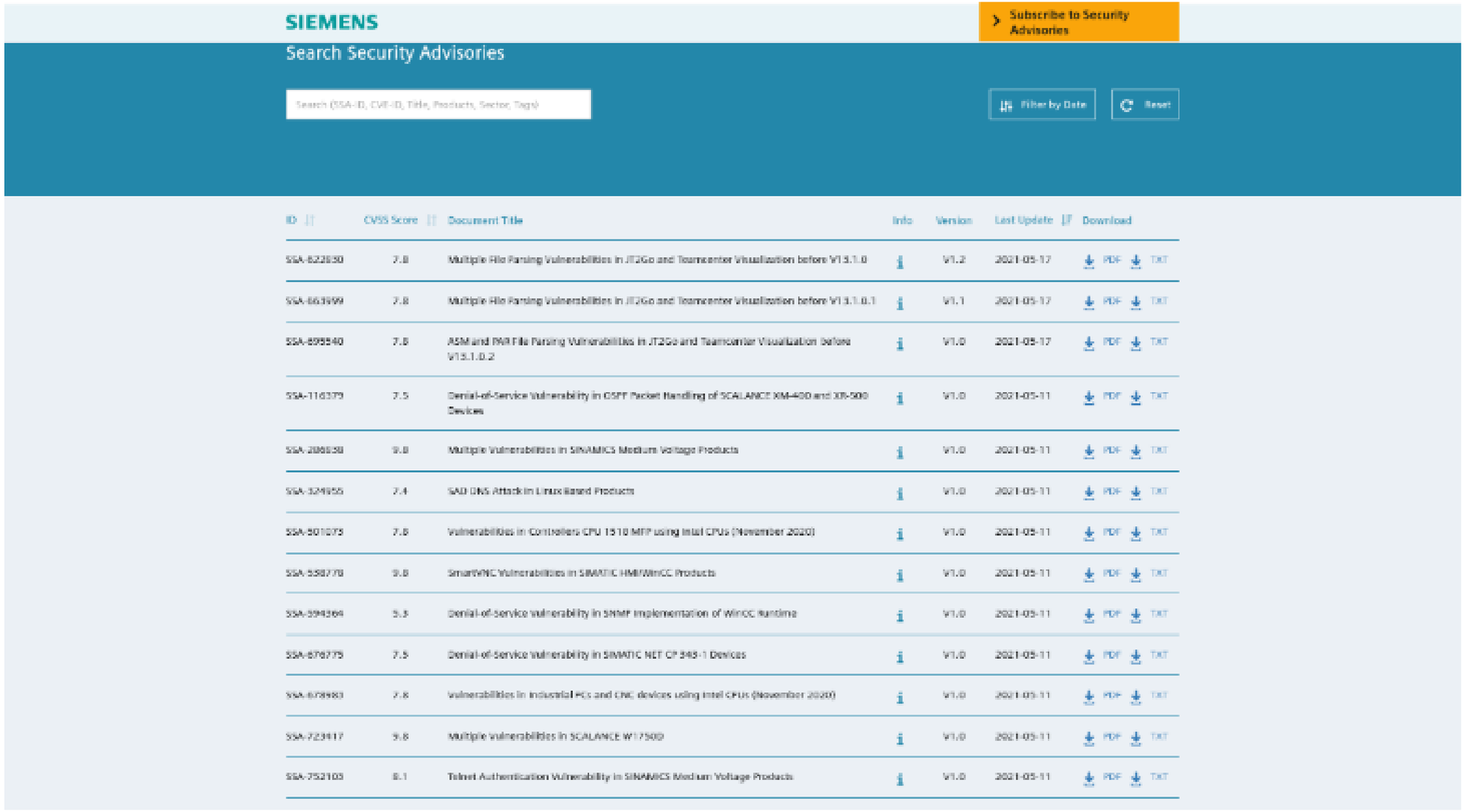
Automatable

Required fields for a VEX

Metadata (author, id, timestamp)	
Product id	Product id
Vulnerability ID Vuln details Product Status Action statement / Impact statement	Vulnerability ID Vuln details Product Status Action statement / Impact statement

Required fields for a VEX





SIEMENS

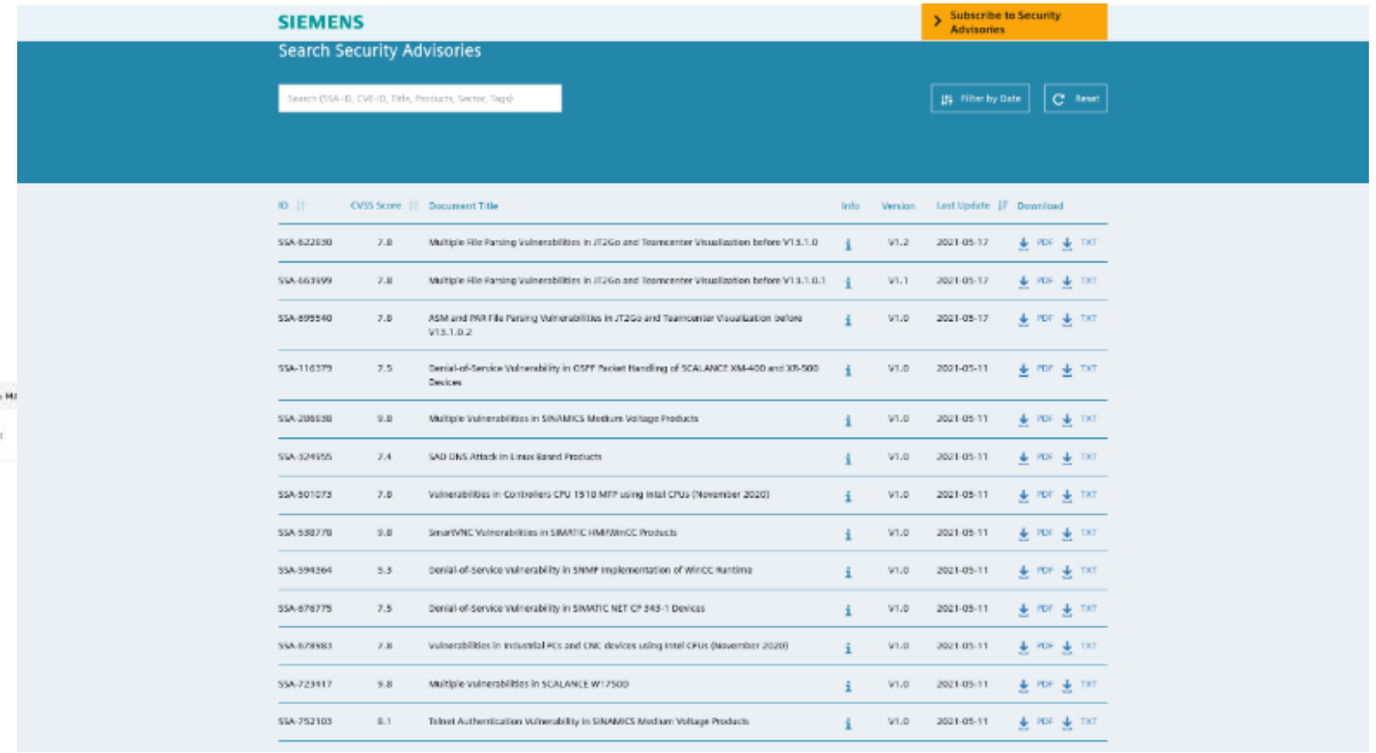
Subscribe to Security Advisories

Search Security Advisories

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

Filter by Date | Reset

ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-622830	7.8	Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.1.0		V1.2	2021-05-17	PDF TXT
SSA-663699	7.8	Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.1.0.1		V1.1	2021-05-17	PDF TXT
SSA-699540	7.8	ASM and PAR File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.1.0.2		V1.0	2021-05-17	PDF TXT
SSA-116379	7.5	Denial-of-Service Vulnerability in OSPF Packet Handling of SCALANCE XM-400 and XR-500 Devices		V1.0	2021-05-11	PDF TXT
SSA-288658	9.8	Multiple Vulnerabilities in SINAMICS Medium Voltage Products		V1.0	2021-05-11	PDF TXT
SSA-324955	7.4	SAD DNS Attack in Linux Based Products		V1.0	2021-05-11	PDF TXT
SSA-501075	7.8	Vulnerabilities in Controllers CPU 1510 MFP using Intel CPUs (November 2020)		V1.0	2021-05-11	PDF TXT
SSA-550778	9.8	SmartVNC Vulnerabilities in SIMATIC HMI/WinCC Products		V1.0	2021-05-11	PDF TXT
SSA-594364	5.3	Denial-of-Service Vulnerability in SNMP Implementation of WinCC Runtime		V1.0	2021-05-11	PDF TXT
SSA-676775	7.5	Denial-of-Service Vulnerability in SIMATIC NET CP 343-1 Devices		V1.0	2021-05-11	PDF TXT
SSA-678983	7.8	Vulnerabilities in Industrial PCs and CNC devices using Intel CPUs (November 2020)		V1.0	2021-05-11	PDF TXT
SSA-723417	9.8	Multiple Vulnerabilities in SCALANCE W1750D		V1.0	2021-05-11	PDF TXT
SSA-752103	8.1	Telnet Authentication Vulnerability in SINAMICS Medium Voltage Products		V1.0	2021-05-11	PDF TXT


SIEMENS
Subscribe to Security Advisories
Search Security Advisories
Filter by Date
Reset
ID
CVSS Score
Document Title
Info
Version
Last Update
Download

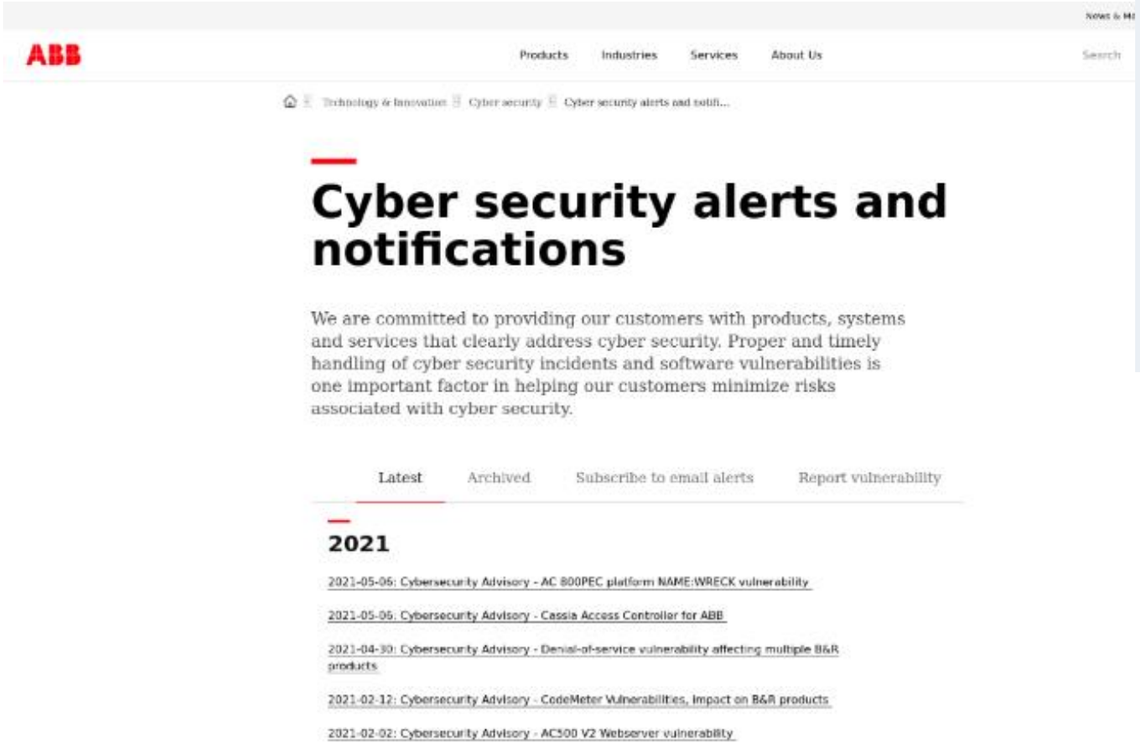
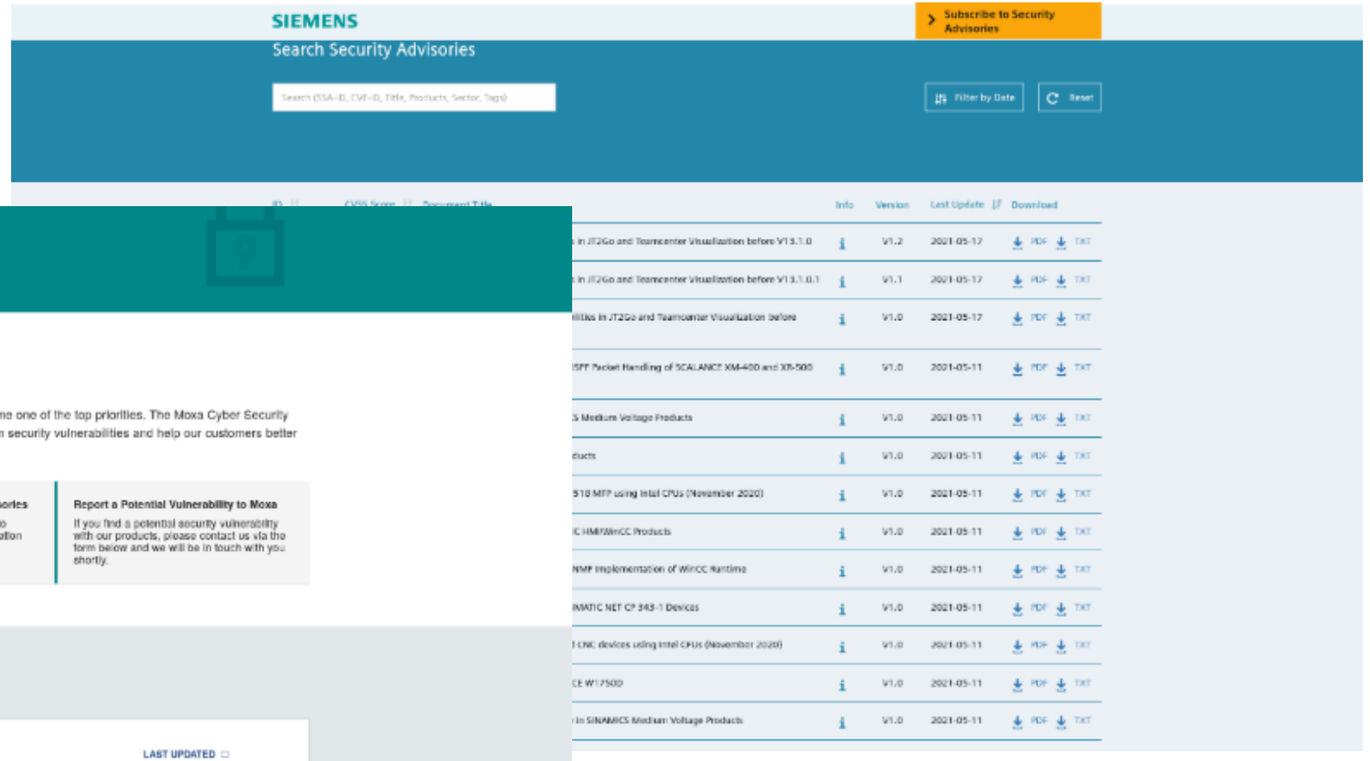
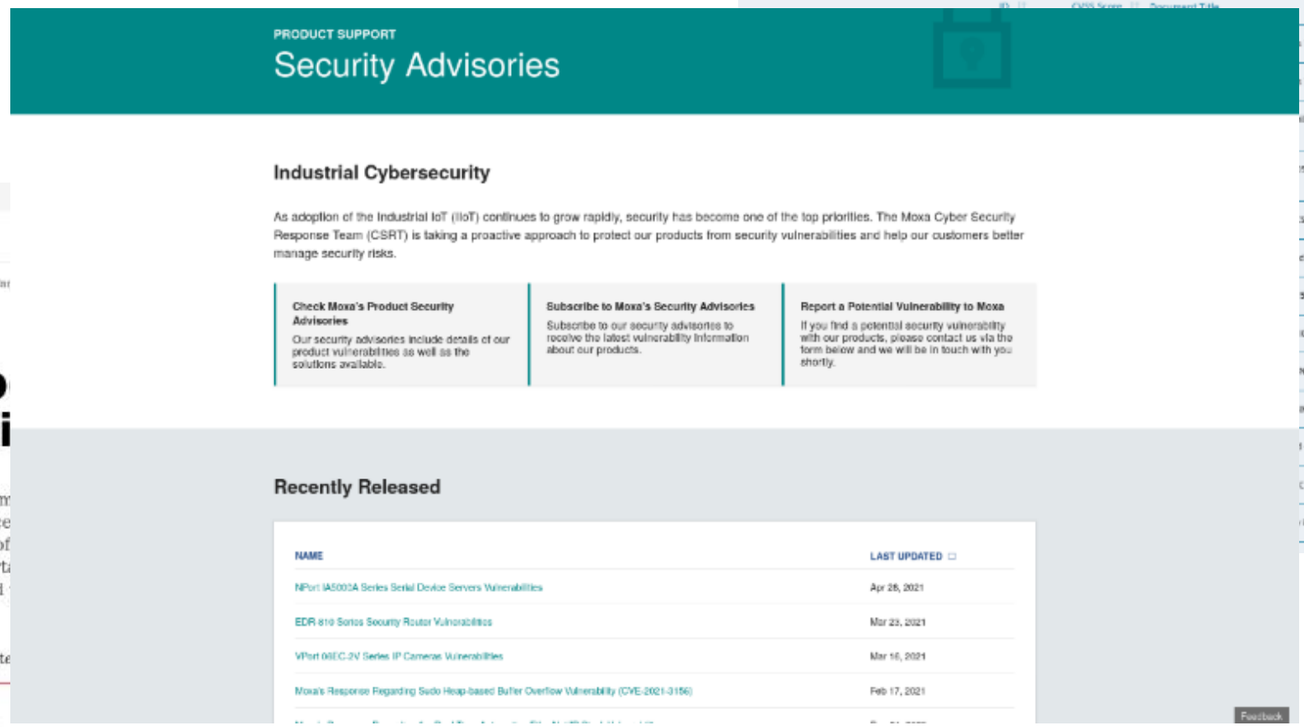


ABB
Products
Industries
Services
About Us
Search
Technology & Innovation
Cyber security
Cyber security alerts and notifi...
Cyber security alerts and notifications
We are committed to providing our customers with products, systems and services that clearly address cyber security. Proper and timely handling 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


SIEMENS
Search Security Advisories
Subscribe to Security Advisories
Filter by Date
Reset
Info
Version
Last Update
Download


PRODUCT SUPPORT
Security Advisories
Industrial Cybersecurity
As adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of the top priorities. The Moxa Cyber Security Response Team (CSRT) is taking a proactive approach to protect our products from security vulnerabilities and help our customers better manage 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.
Report a Potential Vulnerability to Moxa
If you find a potential security vulnerability with our products, please contact us via the form below and we will be in touch with you shortly.
Recently Released
NAME
LAST UPDATED
NPort IA5000A Series Serial Device Servers Vulnerabilities
Apr 28, 2021
EDR-810 Series Security Router Vulnerabilities
Mar 23, 2021
VPort 06EC-2V Series IP Cameras Vulnerabilities
Mar 16, 2021
Moxa's Response Regarding Sudo Heap-based Buffer Overflow Vulnerability (CVE-2021-3156)
Feb 17, 2021
Feedback

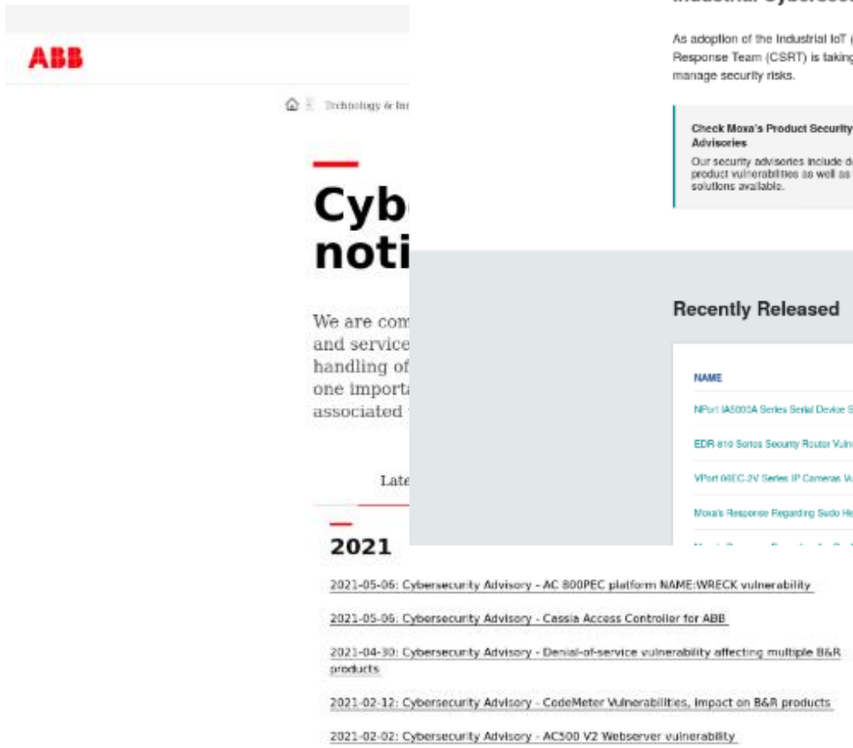
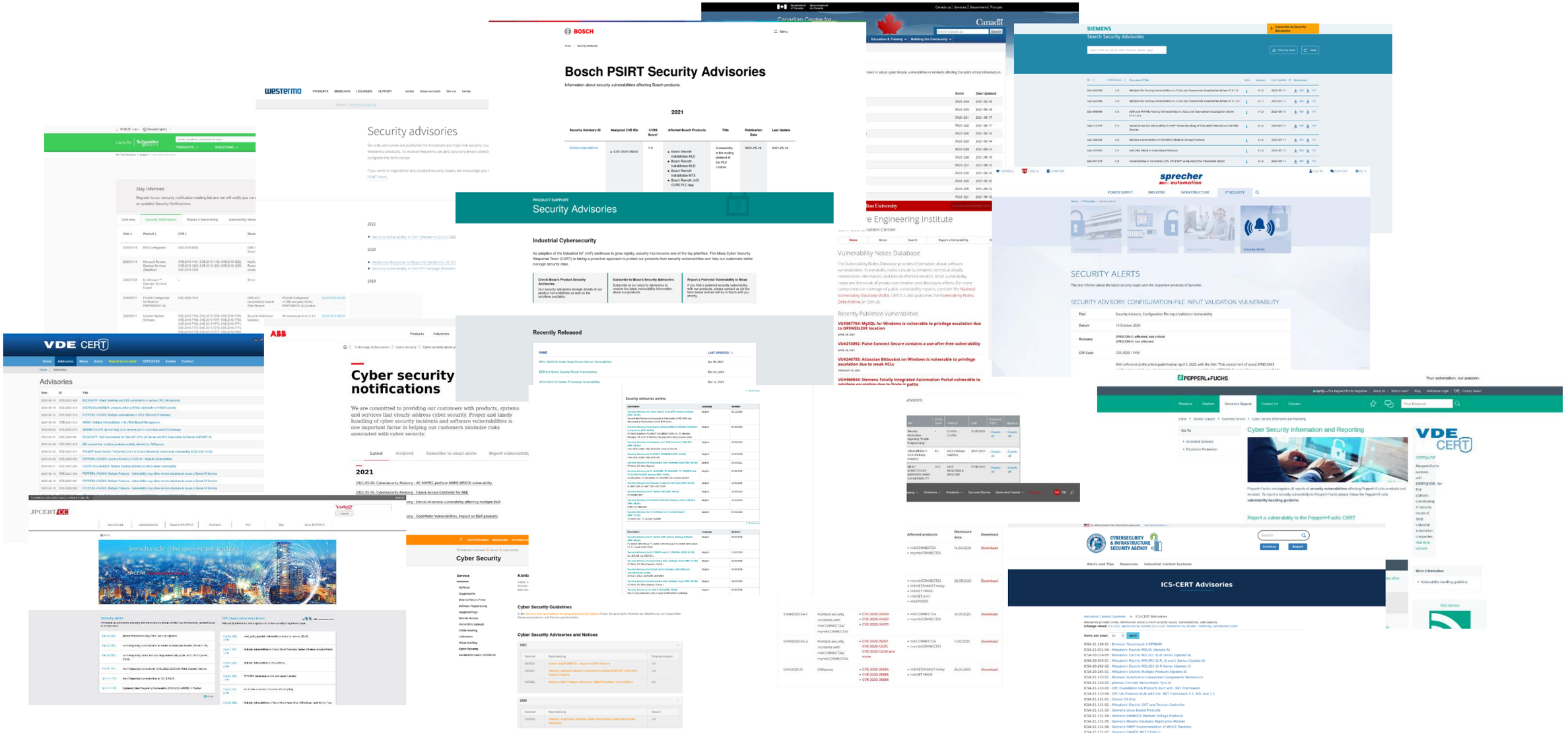
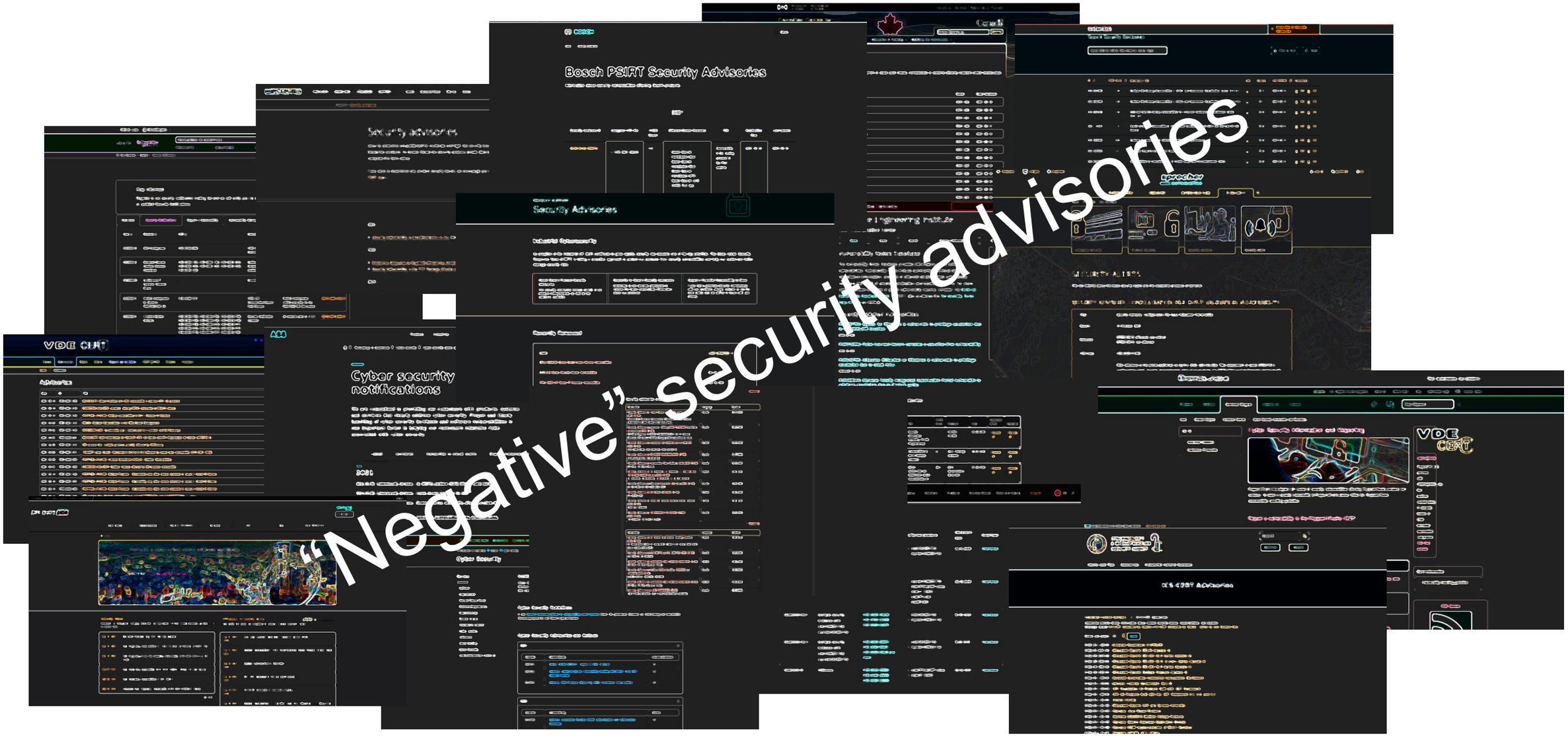


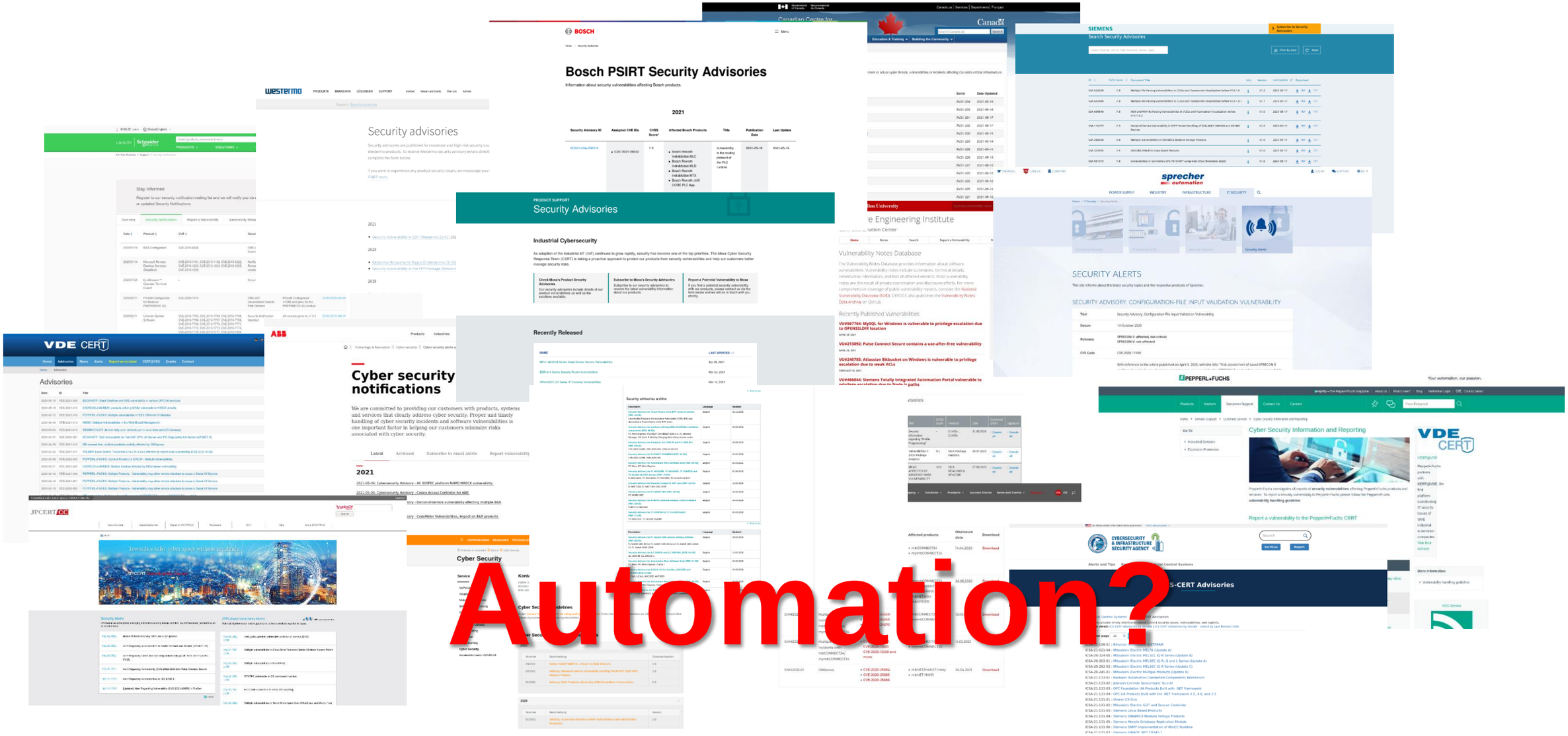
ABB
2021
2021-05-06: Cybersecurity Advisory - AC 800PEC platform NAME:WRECK vulnerability
2021-05-06: Cybersecurity Advisory - Cassia Access Controller for ABB
2021-04-30: Cybersecurity Advisory - Denial-of-service vulnerability affecting multiple B&R products
2021-02-12: Cybersecurity Advisory - CodeMeter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


Bosch PSIRT Security Advisories
Information about security vulnerabilities affecting Bosch products.
2021
Security Advisory ID
Assigned CVE IDs
CVSS Score*
Affected Bosch Products
Title
Publication Date
Last Update
Security Advisories
Industrial Cybersecurity
Recently Released
Vulnerability Notes Database
Recently Published Vulnerabilities
SECURITY ALERTS
SECURITY ADVISORY, CONFIGURATION-FILE INPUT VALIDATION VULNERABILITY
Cyber security 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
Cyber Security
Cyber Security Guidelines
Cyber Security Advisories and Notices
Cyber Security Information and Reporting
Report a vulnerability to the Pepperl+Fuchs CERT
ICS-CERT Advisories


Bosch PSIRT Security Advisories
Security Advisories
Cyber security notifications
VDE CERT
“Negative” security advisories

Security Advisories

https://boyter.org/static/books/CnDD1t0XgAQMXJA.jpg


Bosch PSIRT Security Advisories
Information about security vulnerabilities affecting Bosch products.
2021
Security Advisories
Industrial Cybersecurity
Cyber security 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.
Advisories
Cyber Security
Cyber Security Information and Reporting
ICS-CERT Advisories
Automation?

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 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 Sensiti 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

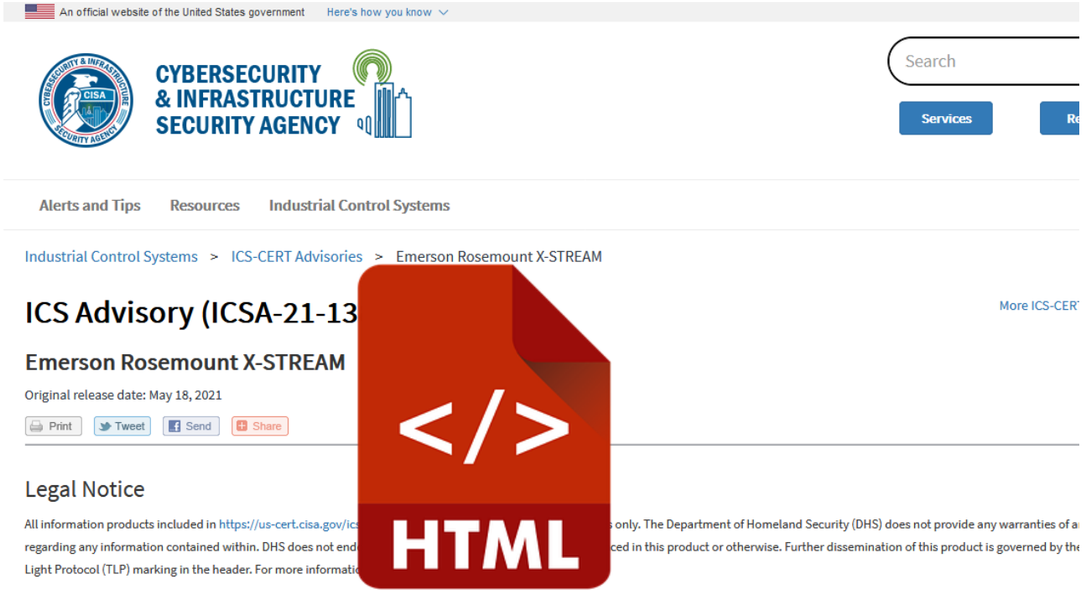
Geo SCADA Expert 2020 April 2021 (83.7787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here:

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.
```



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-21-13

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 only. The Department of Homeland Security (DHS) does not provide any warranties of a regarding any information contained within. DHS does not end ced in this product or otherwise. Further dissemination of this product is governed by the Light Protocol (TLP) marking in the header. For more informati

HTML

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 Sensiti 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 re

Failure to apply the may risk the revealing of account credentials, which could result

Affected Produc

- ClearSCAD
- EcoStruxur
- EcoStruxur and prior

Vulnerability De

CVE ID: CVE-202

CVSS v3.1 Base S L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-916: Use utational Effort* vulnerability exists that could ca s 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.

PDF

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.

11-May-21 Document Reference Number – SEVD-2021-130-07 Page 1 of 3

-----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 thenticated.

This has impact on WP ng TKIP encryption. The attacker must be in t evice to perform the attack.

AFFECTED PRODUCTS AND
=====================

* SCALANCE W1700
  - Affected versions
    All versions <
  - Remediation:
    Update to V1.1
  - Download:
    https://suppor view/109762253

* SCALANCE W700
  - Affected versions
    All versions <
  - 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.

TXT

Machine-readable?

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 Cont 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 re

Failure to apply the may risk the revealing of account credentials, which could result

Affected Produc

- ClearSCAD
- EcoStruxur
- EcoStruxur and prior

Vulnerability De

CVE ID: CVE-202

CVSS v3.1 Base S /PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-916: Use utational Effort* vulnerability exists that could ca s 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

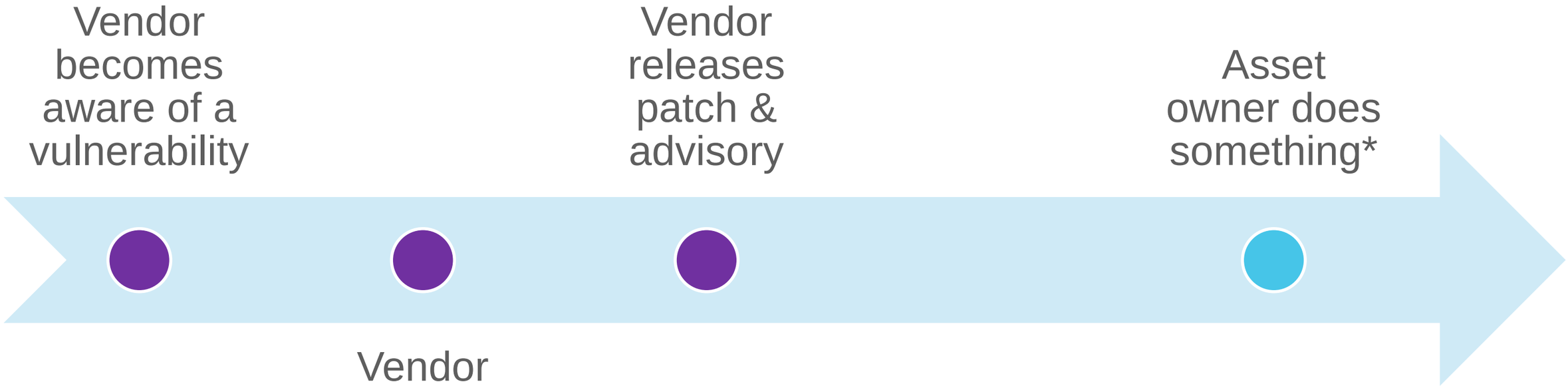
Geo SCADA Expert 2019 (2021) and 2020 (83.7787.1) includes a fix for this vulnerability. The security Expert Downloads

servers. Consult the Release Notes and Resource Center for advice on the procedure.

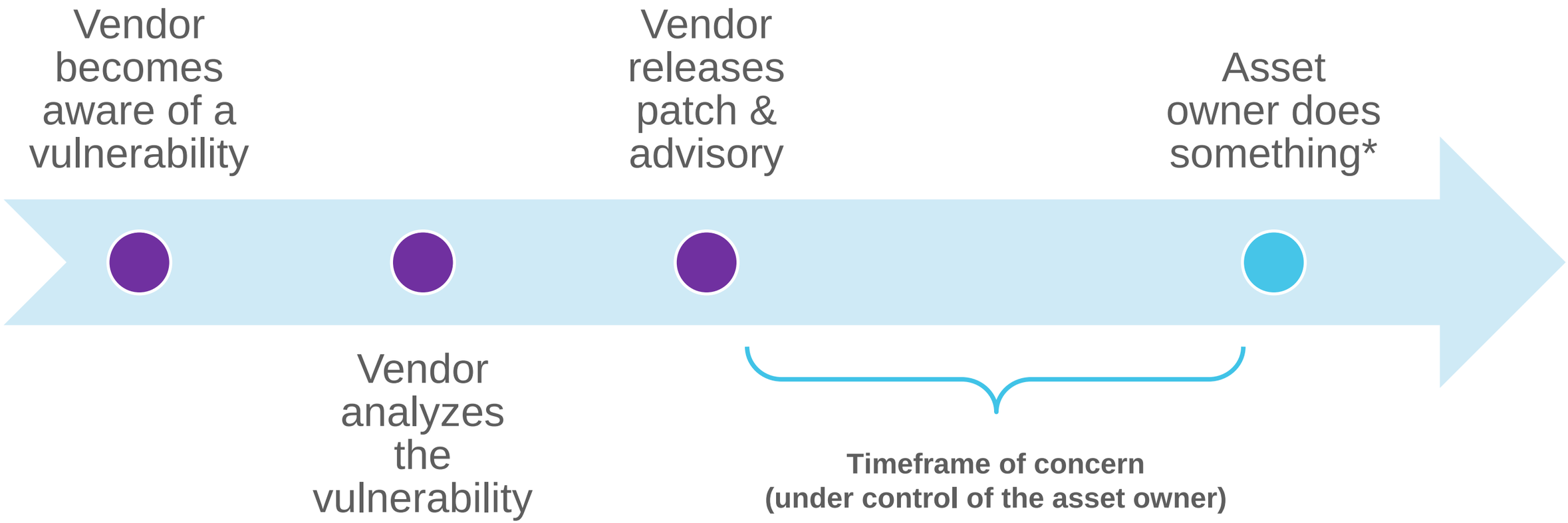
Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure.

```
-----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 thenticated.

This has impact on WP ng TKIP encryption. The
attacker must be in t evice to perform the
attack.

AFFECTED PRODUCTS AND
=====================

* SCALANCE W1700
  - Affected versions
      All versions <
  - Remediation:
      Update to V1.1
  - Download:
      https://suppor view/109762253

* SCALANCE W700
  - Affected versions
      All versions <
  - 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.
```

Human-readable!



* Patch, mitigate risk, or actively accept risk



* Patch, mitigate risk, or actively accept risk

How to automate Security Advisories?

Common Security Advisory Framework (CSAF)

Common Security Advisory Framework

- CSAF 2.0
  - JSON format
  - Machine-readable
  - Build with automation in mind
- Standardization through CSAF TC at OASIS Open
- Successor of CSAF CVRF 1.2

https://boyter.org/static/books/Image-uploaded-from-iOS.jpg

Severity of advisory
- low
- medium
- high
- critical

Vendor

- Production of human-readable advisory
- Publication

Process Today

Severity of advisory
- low
- medium
- high
- critical

User

Vendor

- Production of human-readable advisory
- Publication

Find

- Search websites for new / updated advisories
- Download

Process Today

Severity of advisory
- low
- medium
- high
- critical

User

Vendor
- Production of human-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Prioritize
- Sift criticality of vulnerabilities

Process Today

Severity of advisory
- low
- medium
- high
- critical

User

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 devices?
- Risk assessment
- Decision which actions should be taken

Severity of advisory
- low
- medium
- high
- critical

User

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 devices?
- Risk assessment
- Decision which actions should be taken

Severity of advisory
- low
- medium
- high
- critical

Vendor

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

Severity of advisory
- low
- medium
- high
- critical

Automated

Vendor

- Production of machine-readable advisory
- Publication

Find

- Search websites for new / updated advisories
- Download

Severity of advisory
- low
- medium
- high
- critical

Automated

Vendor

- Production of machine-readable advisory
- Publication

Find

- Search websites for new / updated advisories
- Download

automated

Severity of advisory
- low
- medium
- high
- critical

Automated

Vendor
- Production of machine-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

automated

Evaluate (static)
- Do you have affected devices?

Severity of advisory
- low
- medium
- high
- critical

Automated

Vendor
- Production of machine-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

automated

Evaluate (static)
- Do you have affected devices?

Severity of advisory
- low
- medium
- high
- critical

Automated

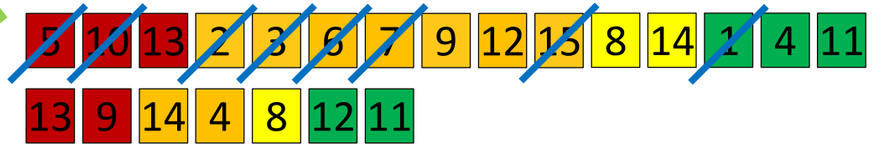
Vendor
- Production of machine-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

automated

Evaluate (static)
- Do you have affected devices?
- Risk assessment (static) => adopt criticality
- Sort by adopted criticality of the vulnerability

automated



Severity of advisory
- low
- medium
- high
- critical

Automated

Vendor
- Production of machine-readable advisory
- Publication

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

Find
- Search websites for new / updated advisories
- Download

automated

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

Evaluate (static)
- Do you have affected devices?
- Risk assessment (static) => adopt criticality
- Sort by adopted criticality of the vulnerability

automated

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

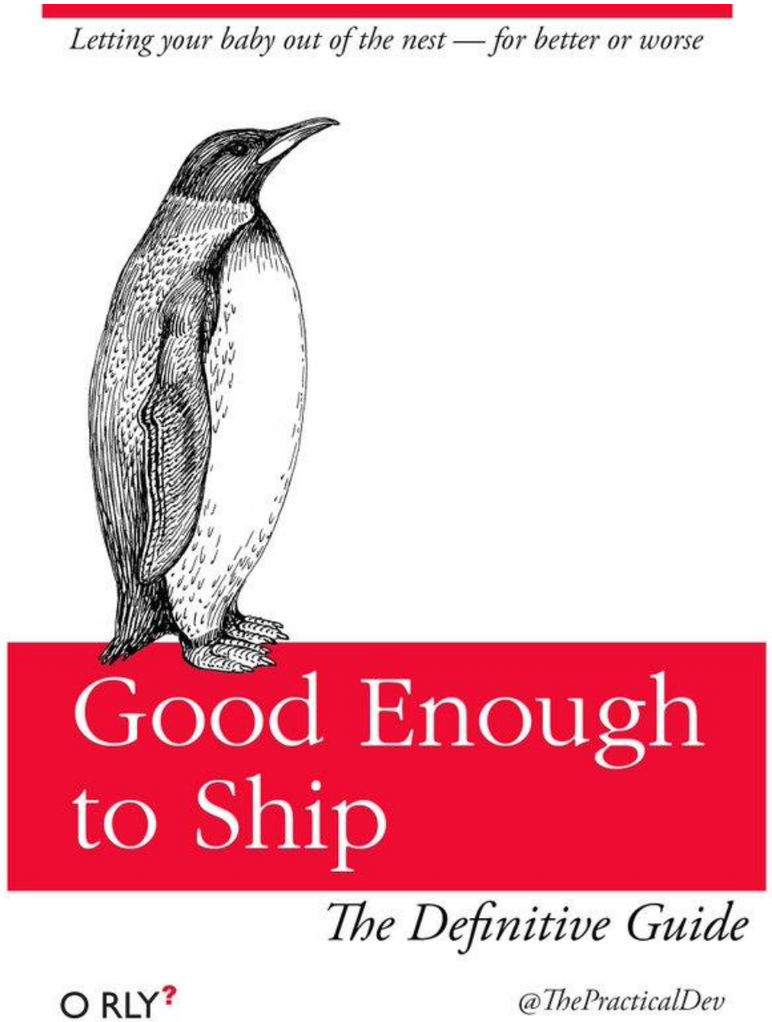
User

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

13 9 14 4 8 12 11

* Patch, mitigate risk, or actively accept risk

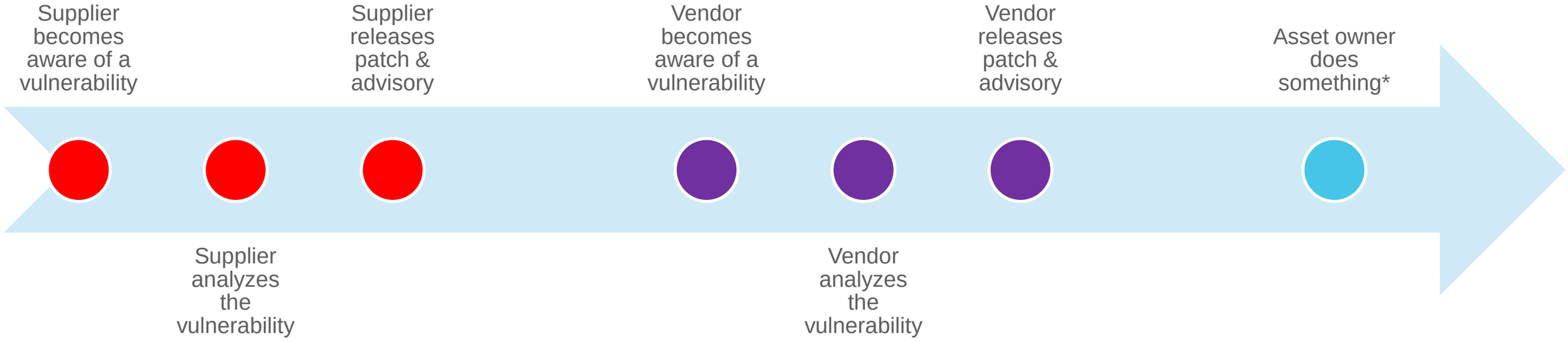
- Reduce human load
  - No more manual searching for advisories
  - Easier to determine affected devices
  - Delegable
  - See only relevant advisories
- Scalable across vendors
- Basic risk assessment based on own environment possible



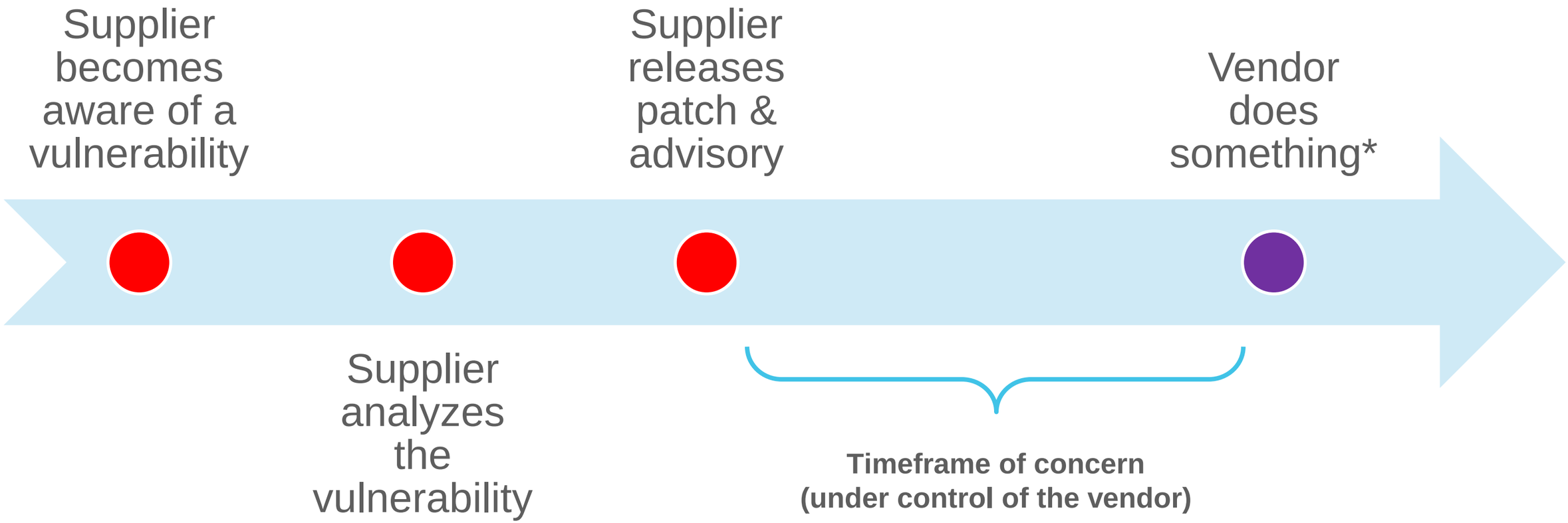
https://boyter.org/static/books/Cg-zWsMWwAEJ-Zn.jpg

How does that help in the supply chain?

Every supplier is a user.



* Patch, mitigate risk, or actively accept risk

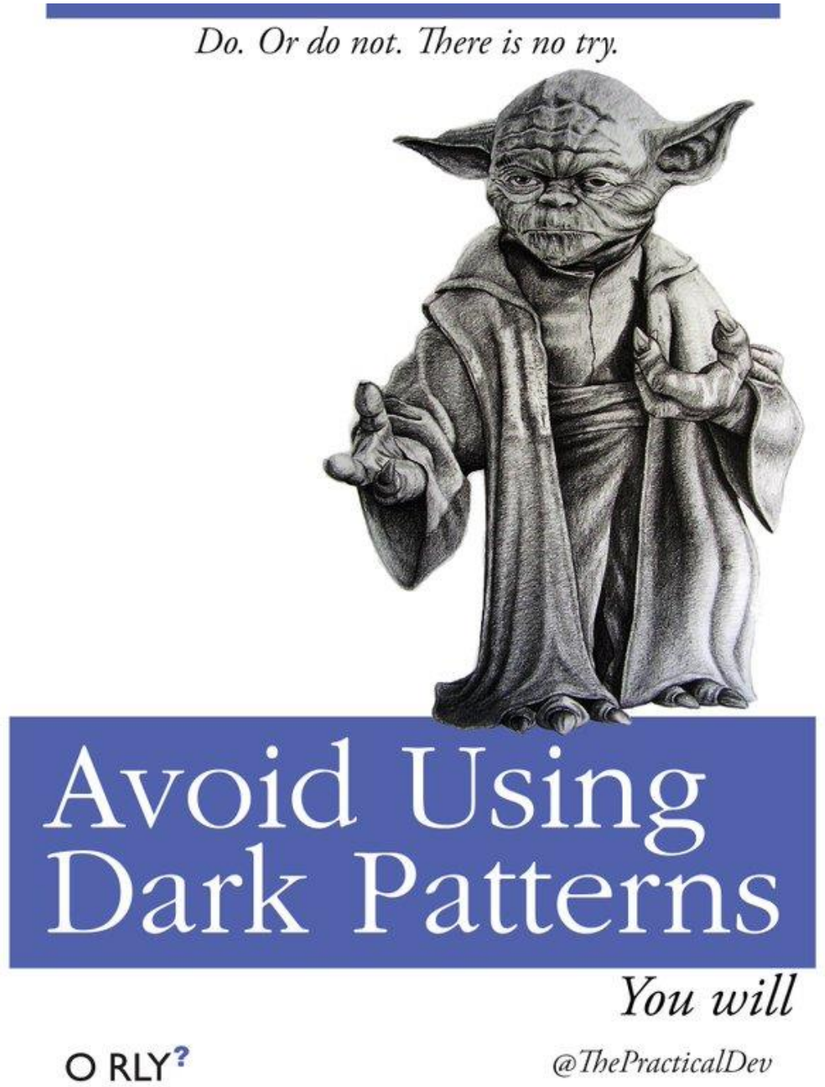


* Analyze, patch & release advisory

- Reduce human load
  - No more manual searching for supplier advisories
  - Easier to determine affected devices
  - Delegable
  - See only relevant advisories
  - Automate advisory creation
- Scalable across supplier
- Basic risk assessment based on own products possible (SBOM)

What does that mean for VEX?

- VEX becomes a profile in CSAF
- Uses same infrastructure and systems



https://boyter.org/static/books/ChnManpWwAANzGq.jpg

Good little product security team does the work to determine whether or not affected.

They are already do this – so help them by make this information public.
And reward them…

Straight from the source*

(*source may vary)


Starting to implement this today
Photo by Matías Ramos on Unsplash

Alright! Problem solved!

Alright! Problem solved?

No. We still need your support to make it work.

Putting off critical tasks until everyone forgets about them

Getting Around to Security Next Month

If there's time

O RLY?

@ThePracticalDev

https://boyter.org/static/books/C3cX4w5VcAENYA7.jpg

1. Request your suppliers to provide advisories in CSAF
2. Provide CSAF documents to your customers to ease their pain
3. Spread the word! #VEX #oCSAF #advisory

(and, yes, #SBOM)

Number of vulnerabilities discovered is rising
Better insights in supply chain
} More advisories

- Advisories are needed for risk-based decisions
- Manual processes don’t scale
- Automation is possible – so automate the boring stuff
- Publish also “known not affected” to reduce questions at support hotline

Come help! (or offer constructive criticism)

CSAF – csaf.io
thomas.schmidt@bsi.bund.de

VEX – ntia.gov/SBOM
afriedman@ntia.gov
@allanfriedman