



# Processi a tool per la gestione delle vulnerabilità di prodotti automotive

## A tier-1 perspective

Automotive SPIN - November 18th, 2021

C. Senni Guidotti Magnani – Connected Vehicle Cyber Security  
L. Bertoglio – Chief Information Security Officer

## UNECE WP.29 R155

### Regulation UNECE WP.29 R155

- Automotive **Framework for Cyber Security Management** – OEMs must be certified by authority;
- Applicable to UNECE Countries and Japan;
- Guidelines for type approval for Company Cyber Security Management;
- Guidelines for vehicle Cyber Security type approval (OEM oriented).

**Vehicle Type** means a category of vehicles which do not differ from each other in such essential respects as: the dimensions and external shape of the vehicle, the number and position of the devices, and other characteristics.

**January 2021:**  
Regulation came into force;  
Japan applies this Regulation.

**July 2022:**  
In the European Union, the  
Regulation on Cyber Security is  
mandatory for all new vehicle  
types

**July 2024:**  
In the European Union the  
Regulation on Cyber Security is  
mandatory for all new vehicles  
produced

## UNECE WP.29 R155

### Regulation UNECE WP.29 R155

- Automotive **Framework for Cyber Security Management** – OEMs must be certified by authority;
- Applicable to UNECE Countries and Japan;
- Guidelines for type approval for Company Cyber Security Management;
- Guidelines for vehicle Cyber Security type approval (OEM oriented).

### The regulation requires the framework to cover two distinct areas:

- Manufacturer's Cyber Security processes;
- Vehicles Cyber Security.

### The regulation applies to:

- Vehicles of category M and N (mainly – vehicles with 4 wheels or more with specific load capacities);
- The regulation also applies to other categories if equipped with automated driving functions beyond level 3.



Automotive SPIN 2021

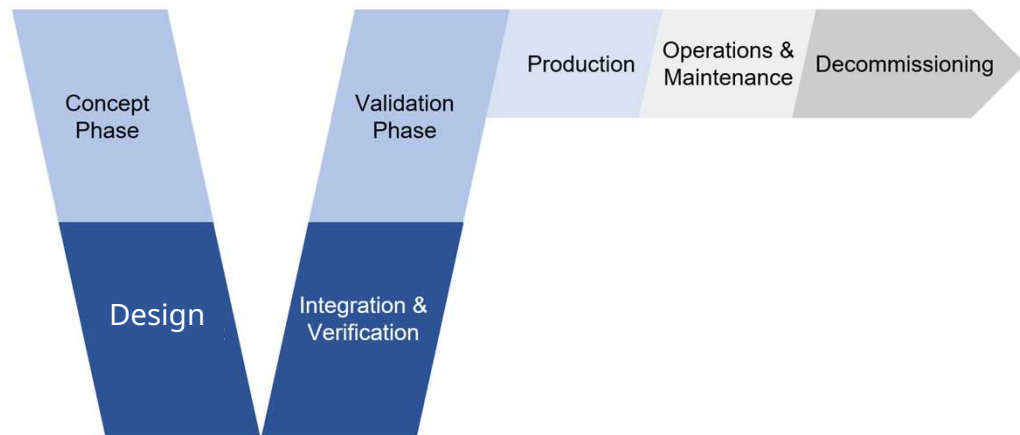


# ISO/SAE 21434 Road vehicles – Cybersecurity engineering

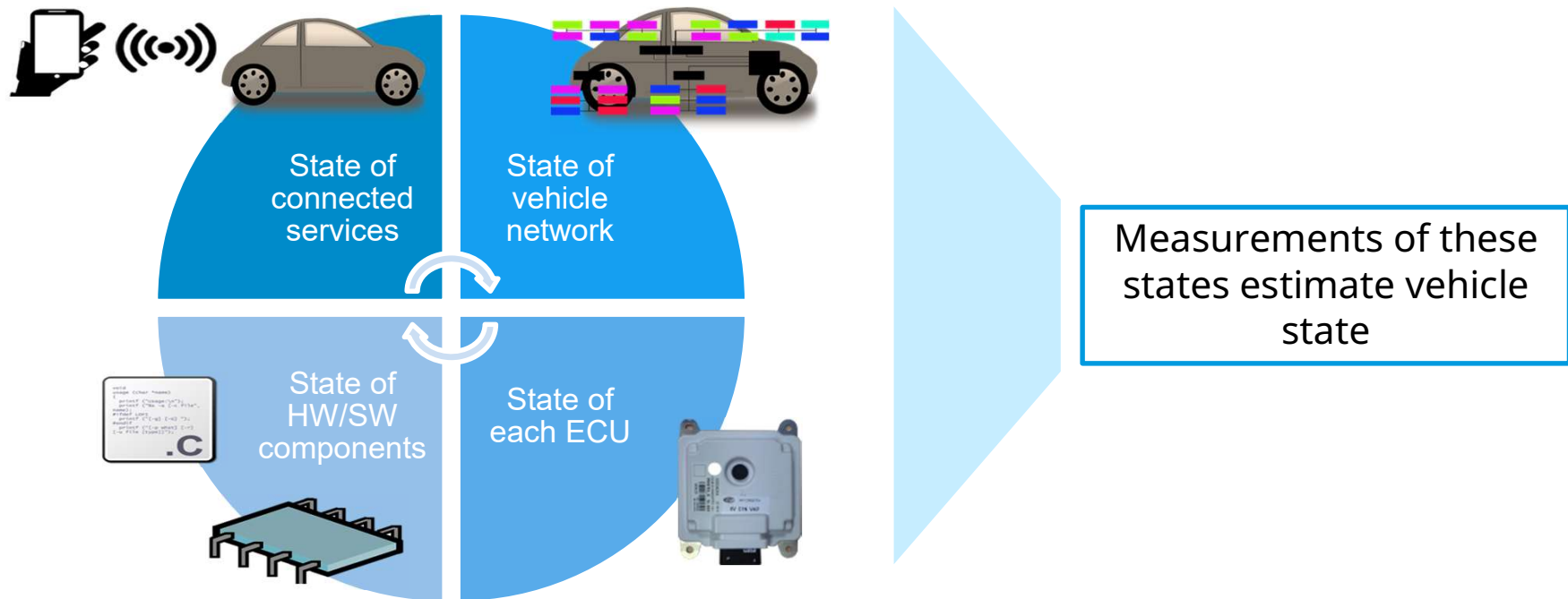
Published 09/2021



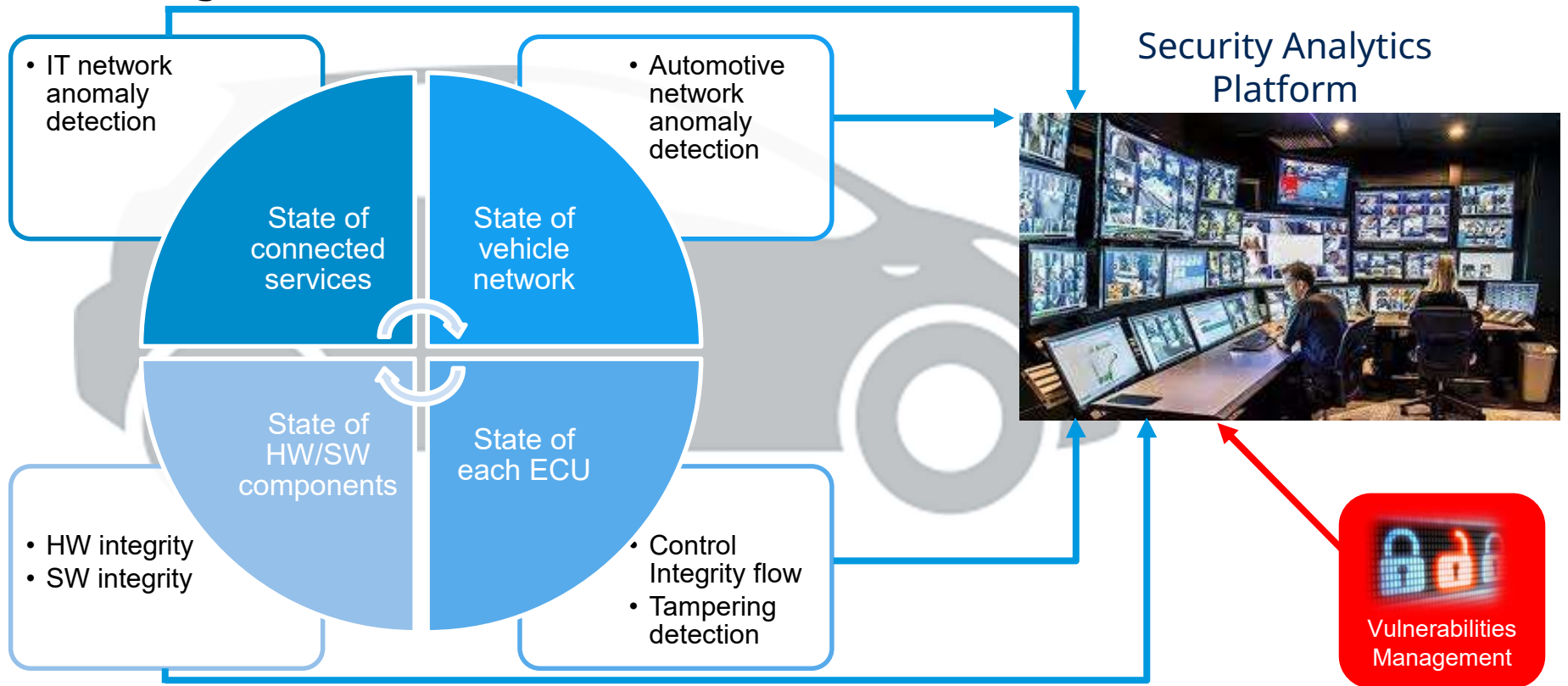
- **ISO/SAE 21434 Road vehicles – Cybersecurity engineering** is the future automotive cyber security development and all related processes.
- The **ISO/SAE 21434** standard brings the Security by Design approach to automotive and ECUs, guiding the definition of framework of documents and processes embracing the entire development and production cycle following this working model



# Vehicle Cyber Security state – WP.29 R155 Monitoring



# Vehicle Cyber Security state - ASOC Technologies





## Vulnerabilities Management for automotive products

UNECE Working Party 29 R155 Cyber Security regulation is requesting to the automotive industry to manage the cyber security risk of its products.

It implies that homologation process of future vehicles will require implementation of Cyber Security processes also to components and parts.

Requirements of WP.29 R155 include (**E.g. Req 7.2.2.2**) the capability of continuously monitoring the presence of known vulnerabilities in the vehicles and thus in their components.

# Some basic notions for vulnerabilities management



## Weakness

issue that can be used to deviate the system from its intended purposes



Common Weakness Enumeration: list of bad practices leading to vulnerable implementations  
<https://cwe.mitre.org/>



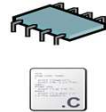
## Vulnerability

specific (i.e. in defined HW and SW) implementation of a weakness



Common Vulnerabilities and Exposures: US public database of vulnerabilities.  
<https://cve.mitre.org/>

## CPE



Common Platform Enumeration: public list and guidelines for unique (almost) identification of HW and SW implementations.  
<https://nvd.nist.gov/products/cpe>

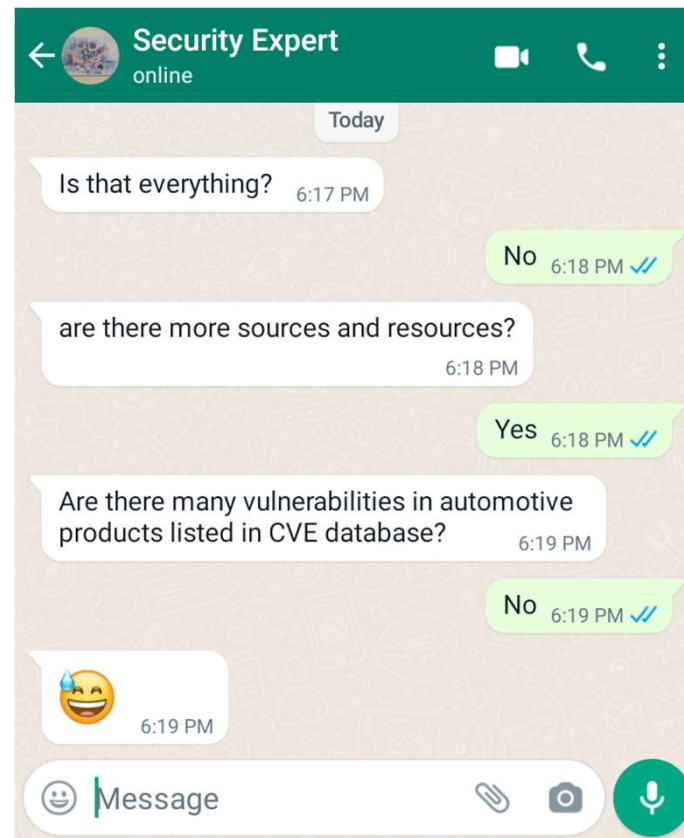


## Exploit / Attack

action leveraging a set of vulnerabilities to reach a goal not originally intended for the system.



# Some basic notions for vulnerabilities management



## Example: Blueborne - simplified



**High Severity**

**5+ billions devices involved**

**Weakness** [CWE-120](#): Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

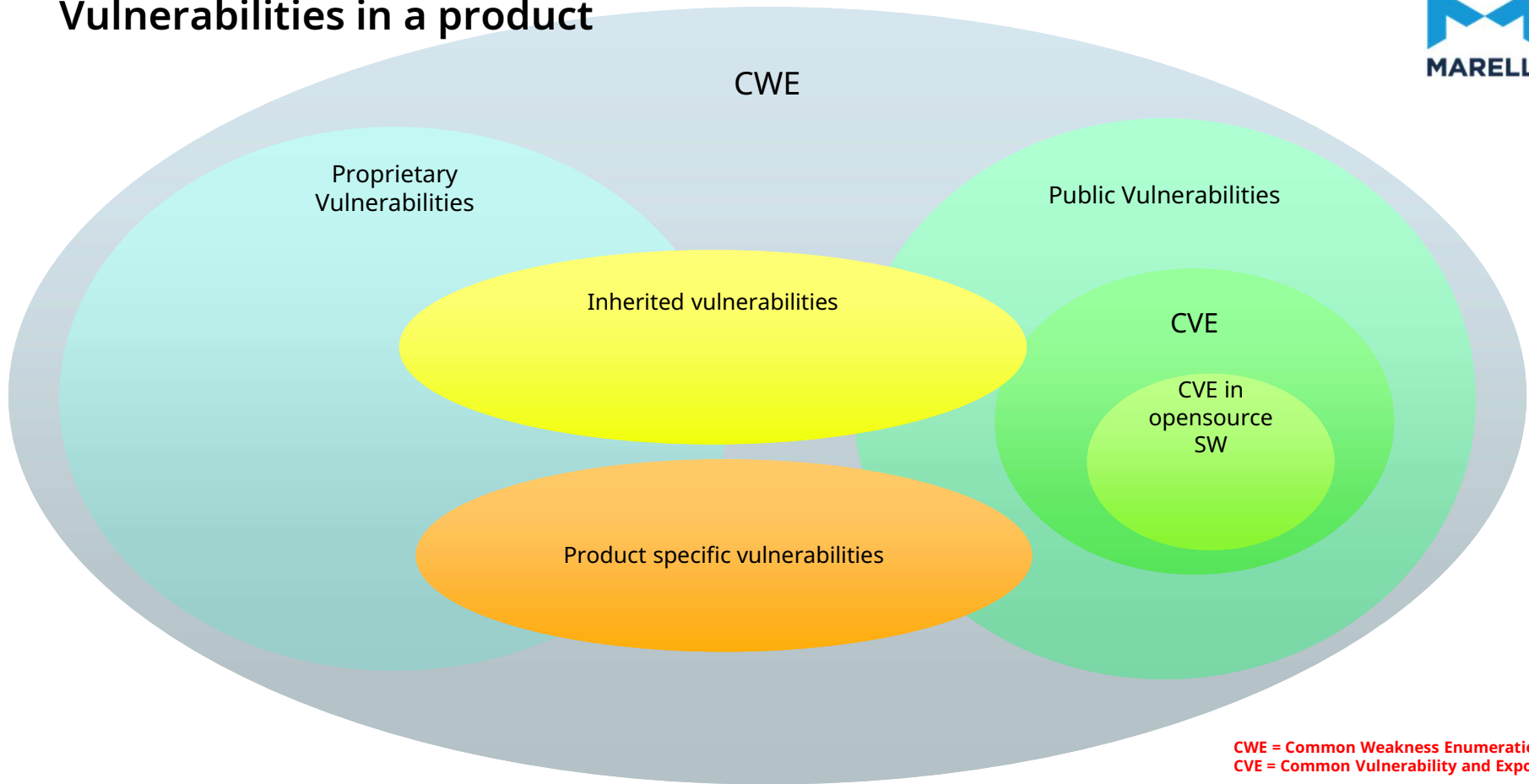
**Vulnerability** CVE-2017-1000251: Linux kernel versions from 3.3-rc1 contain a vulnerable implementation of L2CAP EFS within the BlueZ module.

**Attack:** take control of target Android device

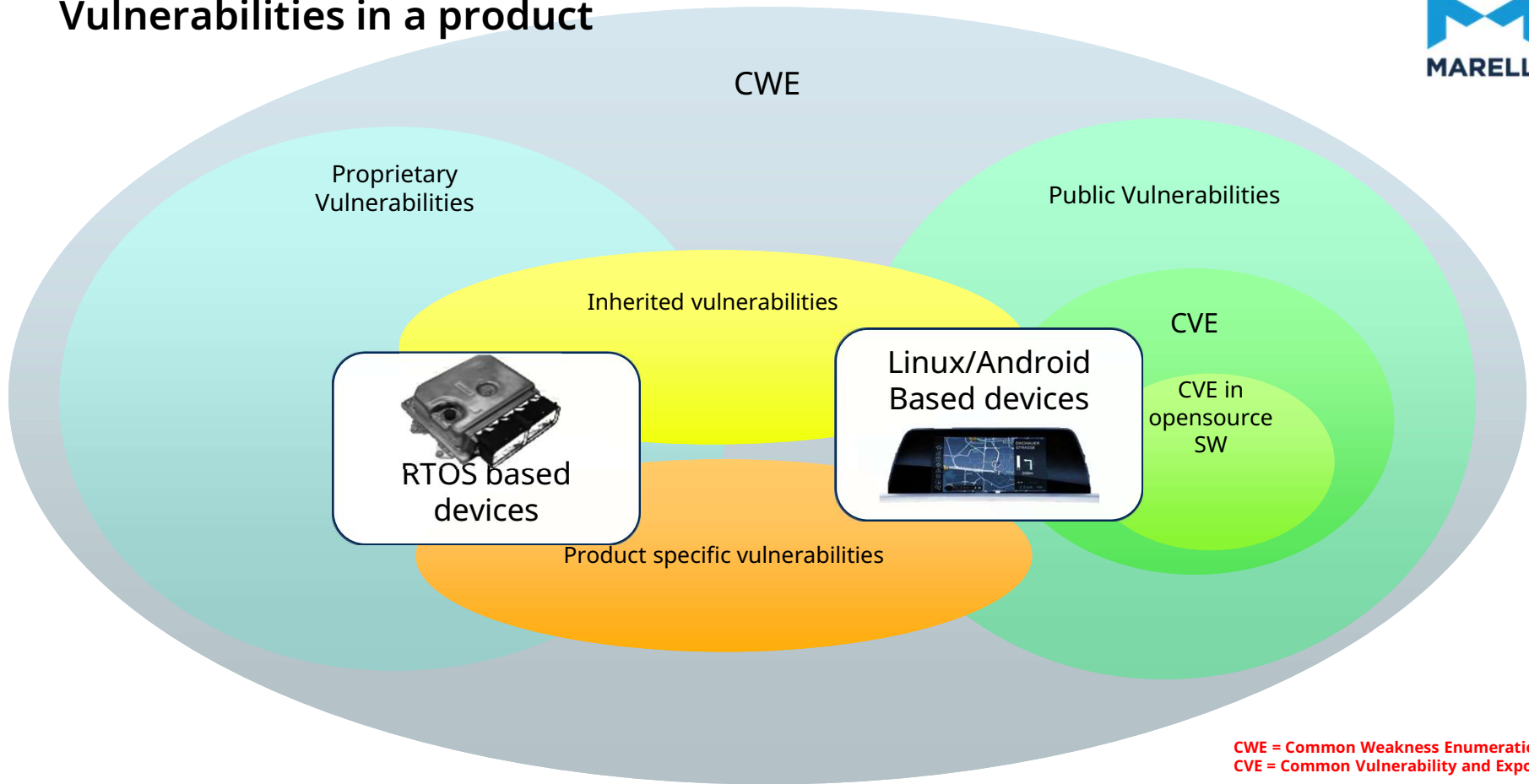
Ref: <https://www.armis.com/blueborne/#/technical>

**CWE = Common Weakness Enumeration**  
**CVE = Common Vulnerability and Exposure**

# Vulnerabilities in a product



# Vulnerabilities in a product



# Is your definition of vulnerability vulnerable?



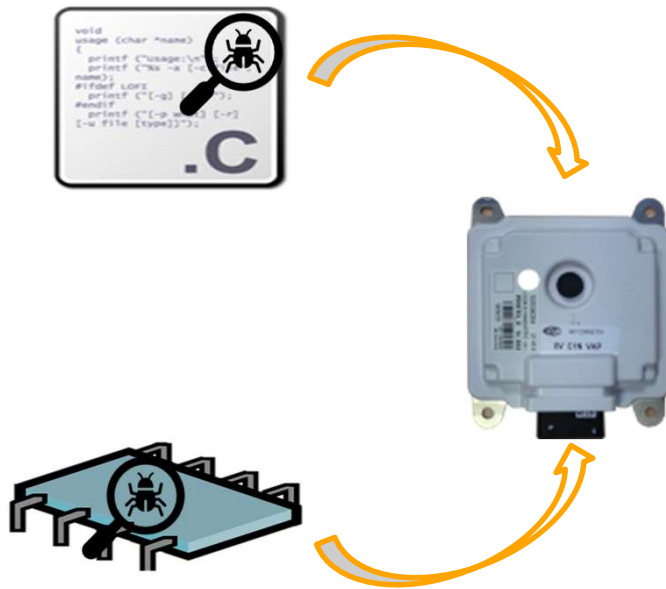
Is it true that your ECU exposes all its private keys in clear text to anyone?

Yeah, but there is no CVE for this!!

Fired!



## Inherited Vulnerabilities – Relations with suppliers



Most products integrate HW and SW components from third parties such as

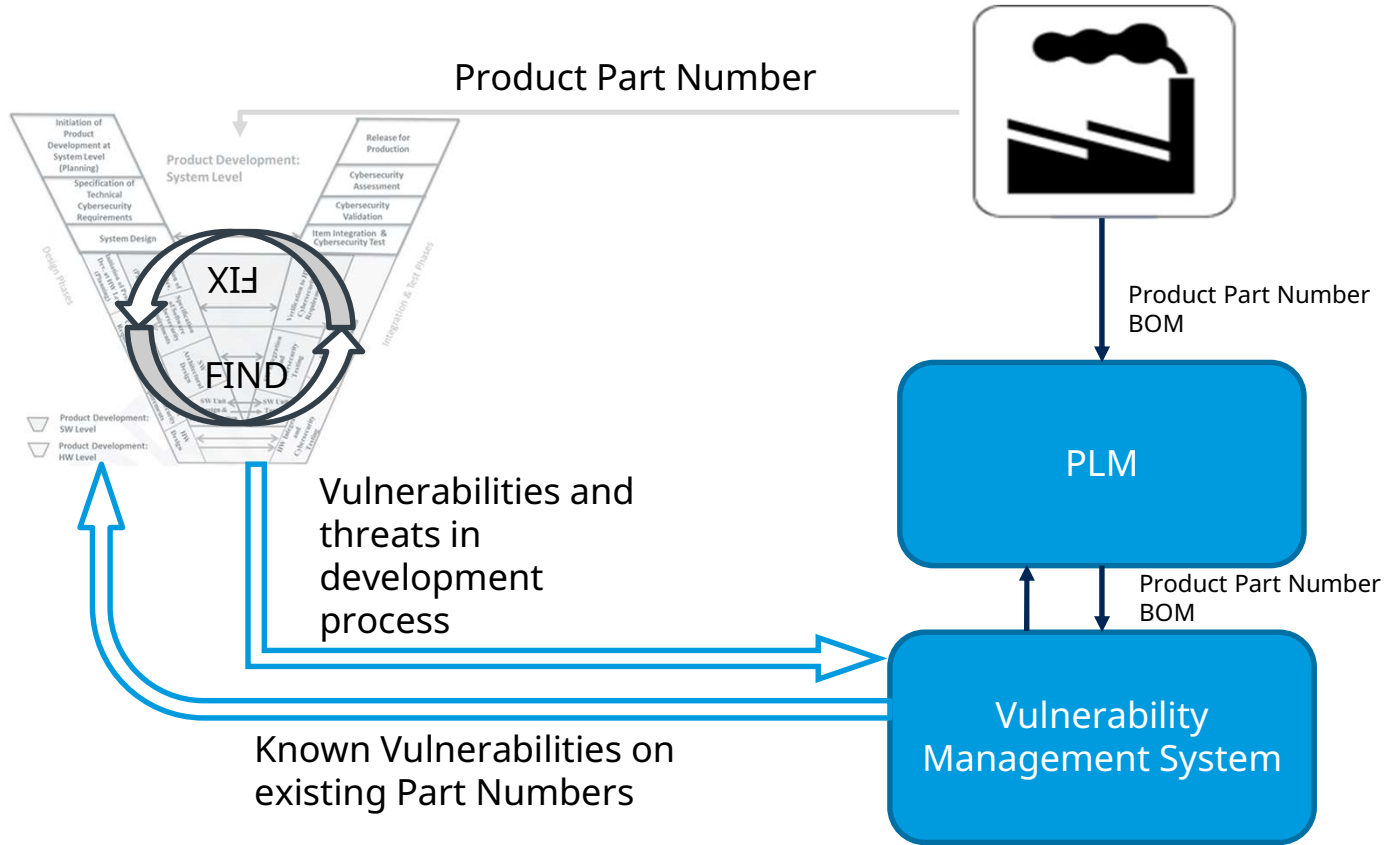
- Open Source communities
- SW suppliers
- HW suppliers providing basic software
- OEM application SW

Vulnerabilities management shall thus be included in Statement Of work and include guidelines to detect and fix vulnerabilities



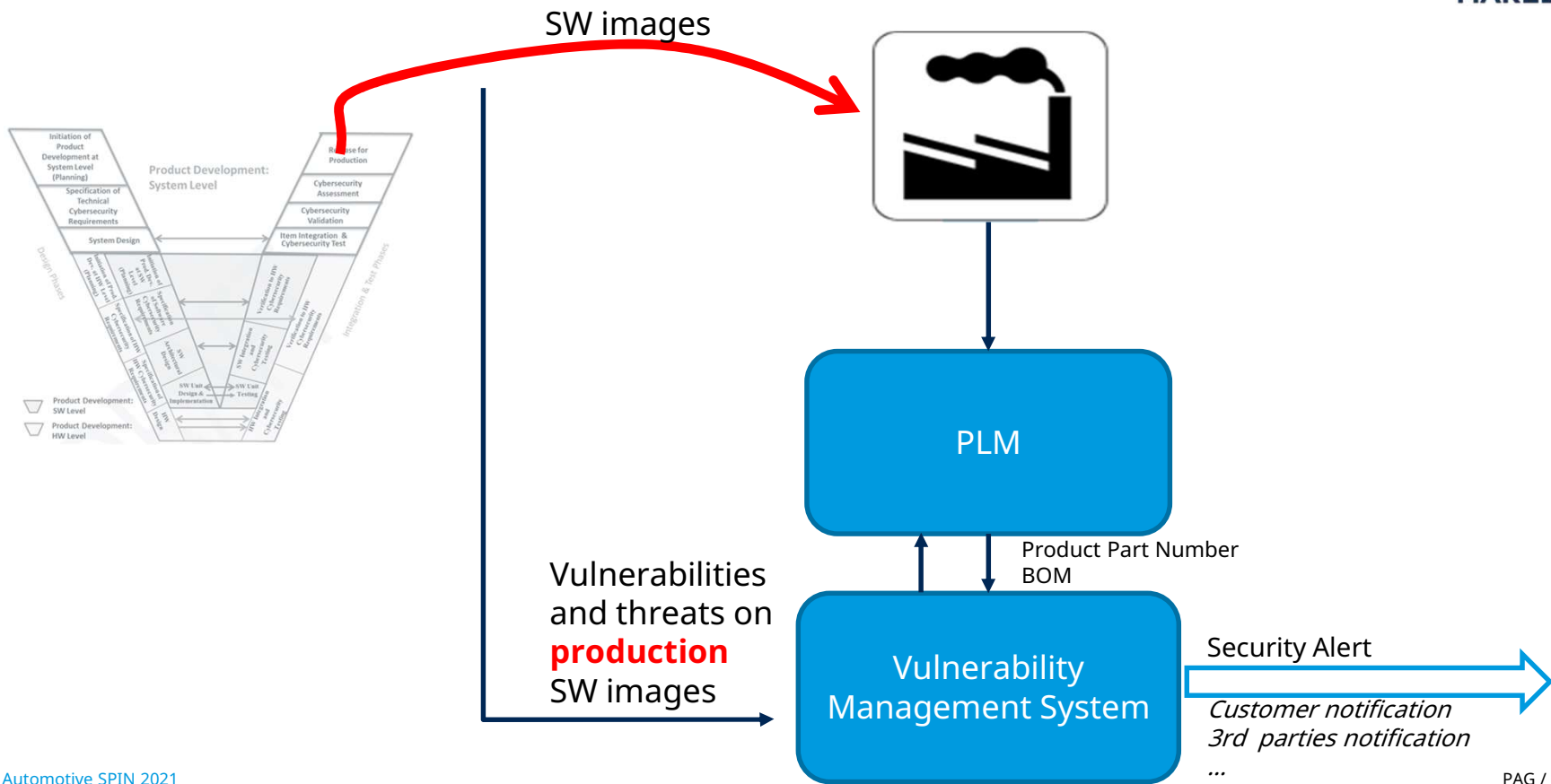
Vulnerabilities Management Workflows

# Vulnerabilities Management – Product Development phase

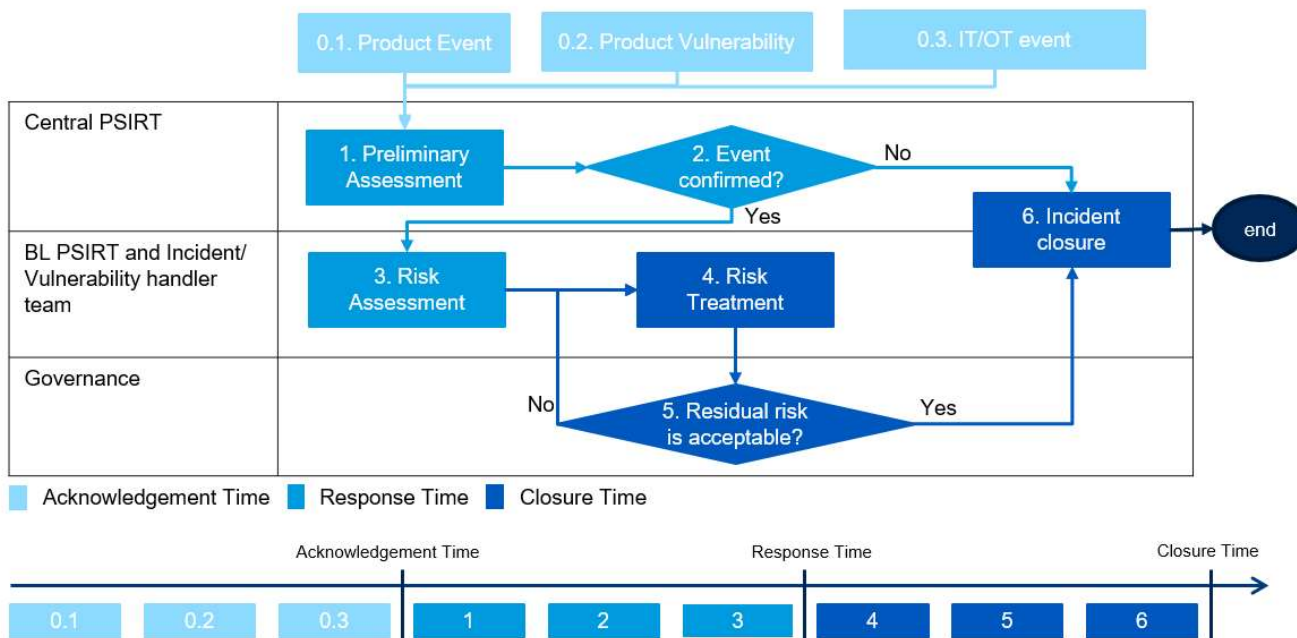




# Vulnerabilities Management – Operation Phase



# What is we manage a vulnerability as an incident? PSIRT Workflows and key facts



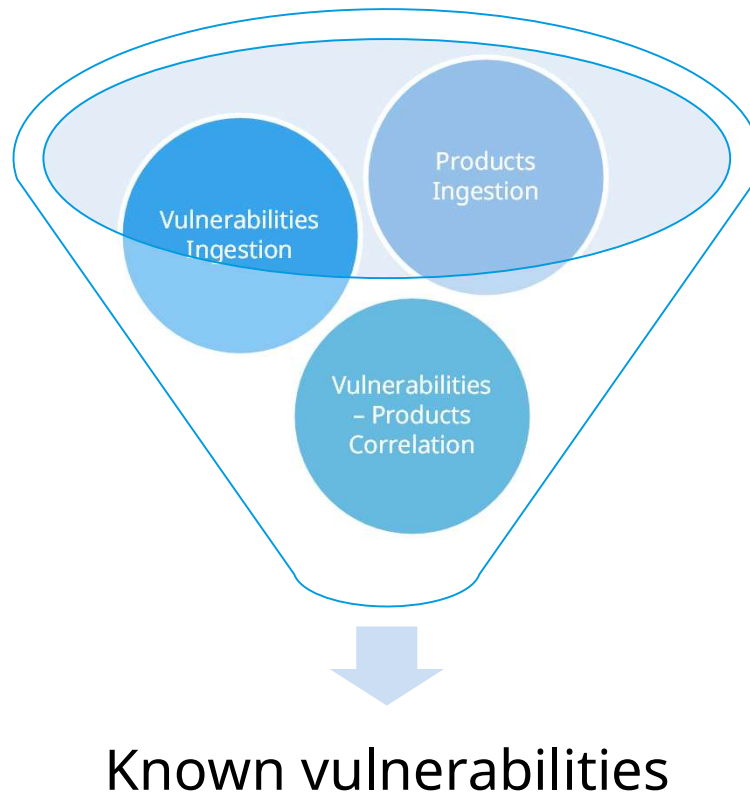
- Marelli PSIRT (Product Security Incident Response Team) is based on two levels of triage, one central and one product specific
- It is integrated with existing Marelli CSIRT
- It provides a 6 items segmentation of incident management on products
- It is based on product specific playbooks
- Incidents prioritization based on risk and agreements with customers



Marelli Vulnerabilities Management System

# Vulnerabilities Management System

## Basic components



- **Vulnerabilities Ingestion:**

- Public sources;
  - NVD
  - JVN
- Auto-ISAC;
- Proprietary sources (simplified list)
  - Specific car-tampering;
  - Findings of VARA and penetration tests run on products.
  - Suppliers

- **Products ingestion:**

- Typically proprietary format stored in PLM system.

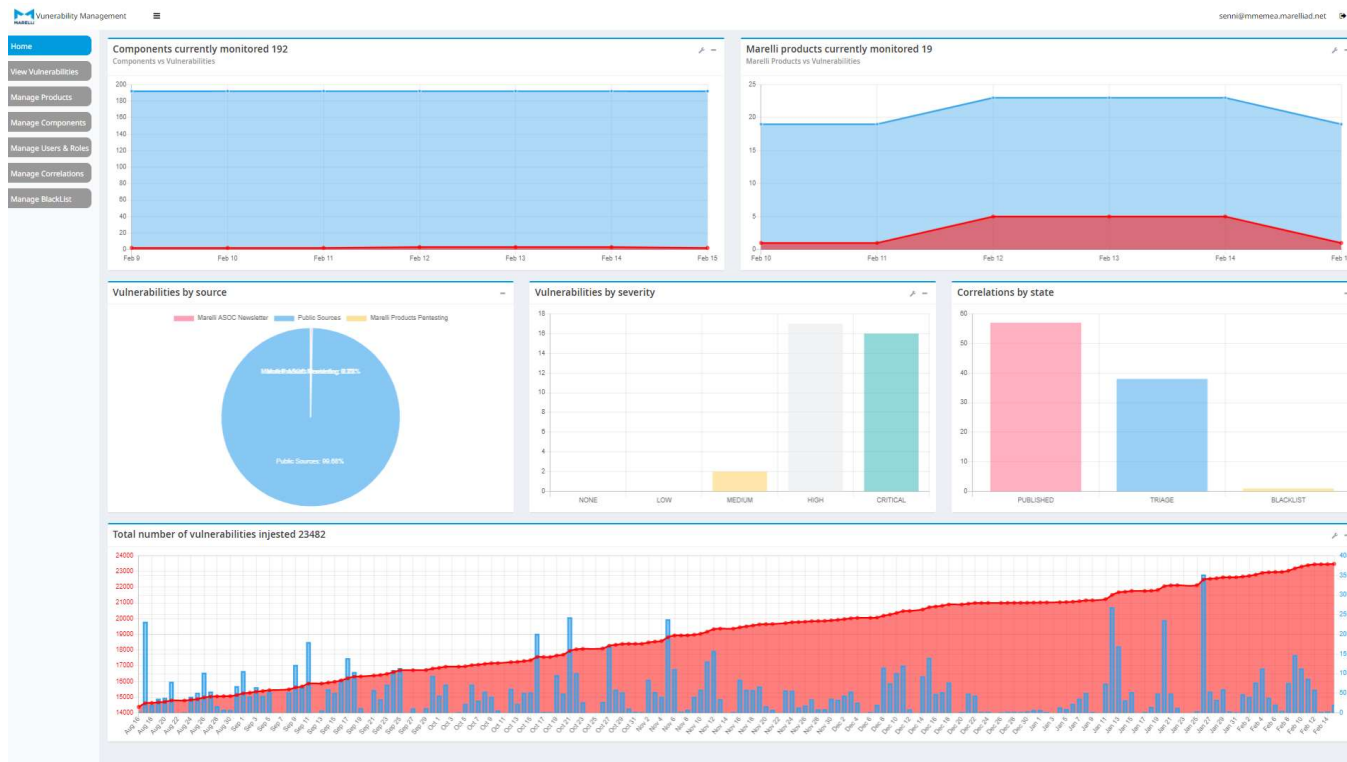
# Products vulnerabilities management



The center of all the system are products.



# Vulnerability Management System for Products



# Vulnerability Management System for Products

## Vulnerabilities DB



### Vulnerabilites page

Vulnerability Management version 1.20210726.3.2  
cosimo.senni@marelli.com

- Home
- Manage Projects
- View Vulnerabilities
- Manage Products
- Manage Components
- Manage Users & Roles
- Manage Correlations
- Manage BlackList

**Choose your filters**

Update Date: Last Week | Year: | Severity: All | Base Score Version: 0 | Source: NVD, Auto-ISAC, Manu...

CVE Identifier Year: | CVE Identifier Suffix: | Vulnerabilities Identifier: | Description: | CWE: | CPE: |

[+ Insert Vulnerability](#) [Reset](#) [Q Search](#)

**Result**

Cve Identifier	Vulnerability Identifier	Description	Severity	Publish Date	Update Date	Number of components associated	Type	Source Type	Associate Component
CVE-2021-34344	MAR-00000005	A stack buffer overflow vulnerability has been reported to affect QNAP device running QUSBCam2. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QUSBCam2: QTS 4.5.4: QUSBCam2 1.1.4 ( 2021/07/30 ) and later QTS 5.0: QUSBCam2 2.0.1 ( 2021/08/03 ) and later QTS 4.3.6: QUSBCam2 1.1.4 ( 2021/07/30 ) and later QTS 4.3.3: QUSBCam2 1.1.4 ( 2021/08/06 ) and later QuTS hero 4.5.3: QUSBCam2 1.1.4 ( 2021/07/30 ) and later	V3.x: 9.8 - V2.0: 7.5	09/10/2021 at 4:15AM	09/23/2021 at 8:54PM	0	PUBLIC	NVD	
CVE-2021-34343	MAR-00000006	A stack buffer overflow vulnerability has been reported to affect QNAP device running QTS, QuTScldoud, QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QTS, QuTScldoud, QuTS hero: QTS 4.5.4.1715 build 20210630 and later QTS 5.0.0.1716 build 20210701 and later QuTScldoud c4.5.6.1755 and later QuTS hero h4.5.4.1771 build 20210825 and later	V3.x: 7.2 - V2.0: 6.5	09/10/2021 at 4:15AM	09/23/2021 at 7:52PM	0	PUBLIC	NVD	
CVE-2021-28816	MAR-00000007	A stack buffer overflow vulnerability has been reported to affect QNAP device running QTS, QuTScldoud, QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QTS, QuTScldoud, QuTS hero: QTS 4.5.4.1715 build 20210630 and later QTS 5.0.0.1716 build 20210701 and later QTS 4.3.3.1693 build 20210624 and later QTS 4.3.6.1750 build 20210730 and later QuTScldoud c4.5.6.1755 and later QuTS hero h4.5.4.1771 build 20210825 and later	V3.x: 8.8 - V2.0: 6.5	09/10/2021 at 4:15AM	09/23/2021 at 5:26PM	0	PUBLIC	NVD	
CVE-2021-28813	MAR-00000008	A vulnerability involving insecure storage of sensitive information has been reported to affect QSW-M2116P-2T2S and QNAP switches running QuNetSwitch. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism. We have already fixed this vulnerability in the following versions: QSW-M2116P-2T2S 1.0.6 build 210713 and later QGD-1600P: QuNetSwitch 1.0.6.1509 and later QGD-1602P: QuNetSwitch 1.0.6.1509 and later QGD-3014PT: QuNetSwitch 1.0.6.1519 and later	V3.x: 7.5 - V2.0: 5.0	09/10/2021 at 4:15AM	09/23/2021 at 3:53PM	0	PUBLIC	NVD	
CVE-2021-34346	MAR-00000003	A stack buffer overflow vulnerability has been reported to affect QNAP device running NVR Storage Expansion. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of NVR	V3.x: 9.8 - V2.0: 7.5	09/10/2021 at 4:15AM	09/23/2021 at 3:50PM	0	PUBLIC	NVD	

# Vulnerability Management System for Products

## Products page



Vulnerability Management version: 1.203.10729.3.2243  
cosimo.senni@marelli.com

- Home
- Manage Projects
- View Vulnerabilities
- Manage Products
- Manage Components
- Manage Users & Roles
- Manage Correlations
- Manage BlackList

**Choose your filters**

Product Part Number  Tags  Product Name

Project

[+ Insert Product](#) [+ Import Product](#) [Reset](#) [Search](#)

**Result**

Product Part Number	Product Name	State	SOP	Tag	Project	Number of Components with vulnerabilities	Modify	Delete
		Production	7/2021		N/A	0		
		Derogato	N/A		N/A	0		
		N/A	N/A		N/A	0		
		N/A	10/2023		Rear Lights	2		
		Working	N/A		N/A	1		
		Working	N/A		N/A	38		

Items per page: 10    1 - 6 of 6    |< < > >|



# Vulnerability Management System for Products

## Product Detail and vulnerabilities



Product details 99999999

Name: Demo

State: N/A

SOP: 10/2023

Tags: Demo

Manufacturing Plant: Barberà del Valles, Barberà del Valles

Markets: APAC, EMEA, EMEA

Description:

Supplier Part Number	Supplier	Number of vulnerabilities associated	Type	Description
APQ-8096AU-0-905FCBGA+H5-MT-01-1-AC	Qualcomm	204	HW	MICROCONTROLLER
cpe:2.3:a:libpng:libpng:1.2.56	libpng	9	SW	libpng
QCA-6564AU-1-169FBGA-TR-07-0	Qualcomm	0	HW	MICROCONTROLLER
cpe:2.3:a:al:pbl:21w14d5	pbl	0	SW	pbl
MPC563XM	NXP	0	HW	Microcontroller MPC56xx family

Items per page: 5 1 - 5 of 16

[Product Vulnerabilities Report](#)



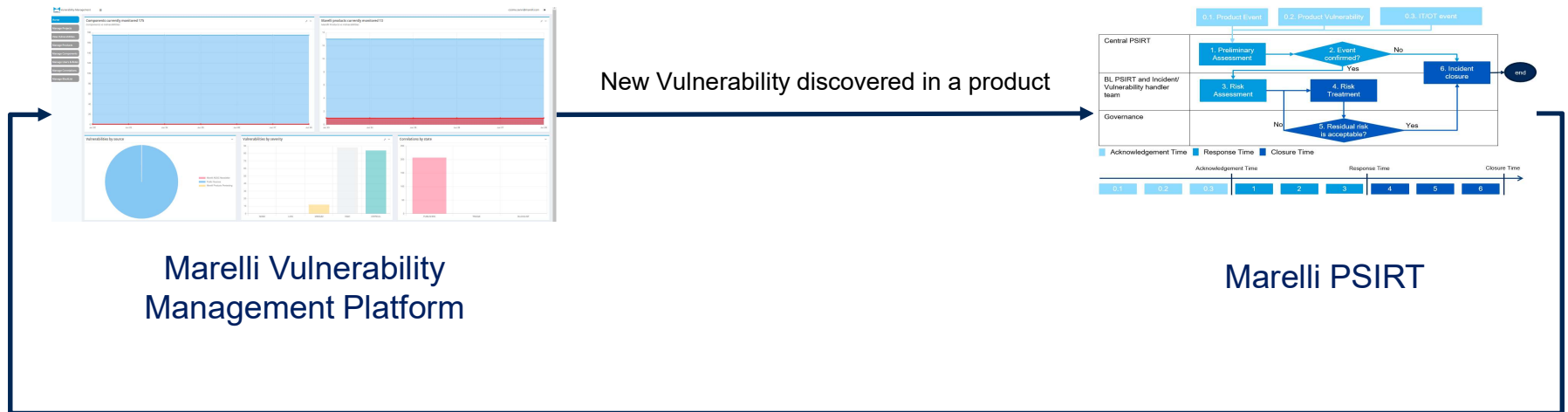
## Marelli Vulnerability Management Platform – Supported Use Cases

- Count total number of vulnerabilities contained in a product
- Select products with specified critical vulnerabilities
- Measure trend of growth of vulnerabilities associated with products
- Identify components with critical vulnerabilities
- Count components with vulnerabilities from a given supplier
- Import and associate to product results of penetration test
- Create and download report with vulnerabilities associated to a product

# Integrated Vulnerability Management Framework



Vulnerabilities on Marelli products are managed as standard incidents. Integration between Marelli Vulnerability Management Platform is planned as described below



Result of incident management on vulnerability (either patched or accepted)