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:

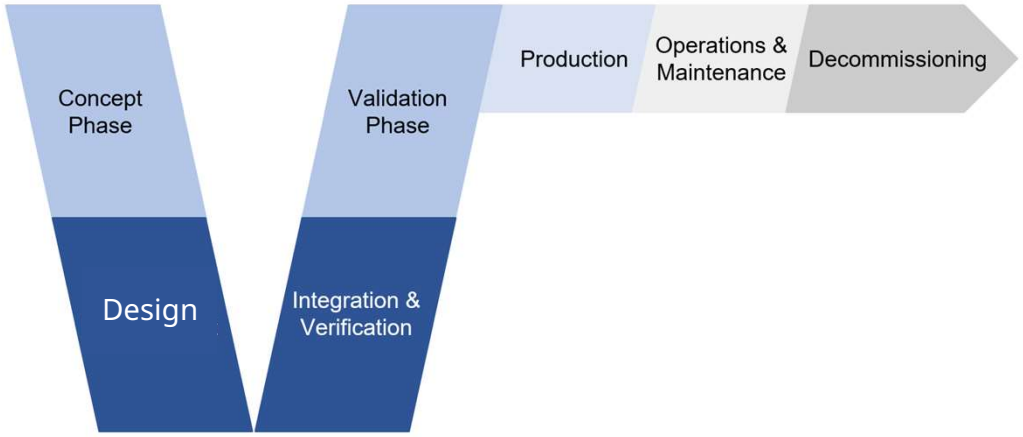
- Vehicles of category M and N (mainly – vehicles with 4 wheels or more with specific load capacities);
- The regulation also applies to other categories if equipped with automated driving functions beyond level 3.



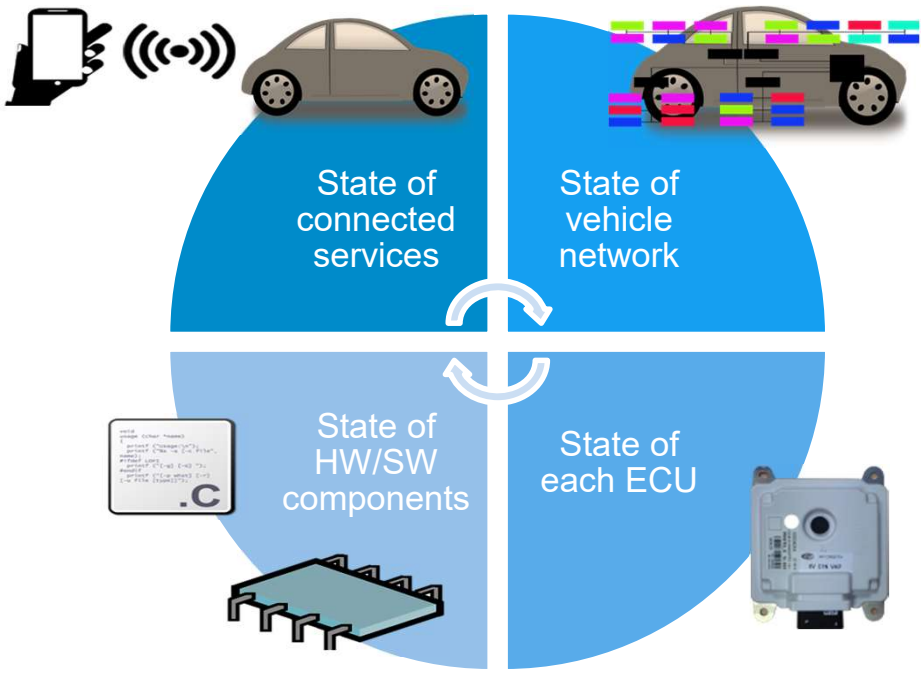


ISO/SAE 21434 Road vehicles – Cybersecurity engineering
Published 09/2021

- **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

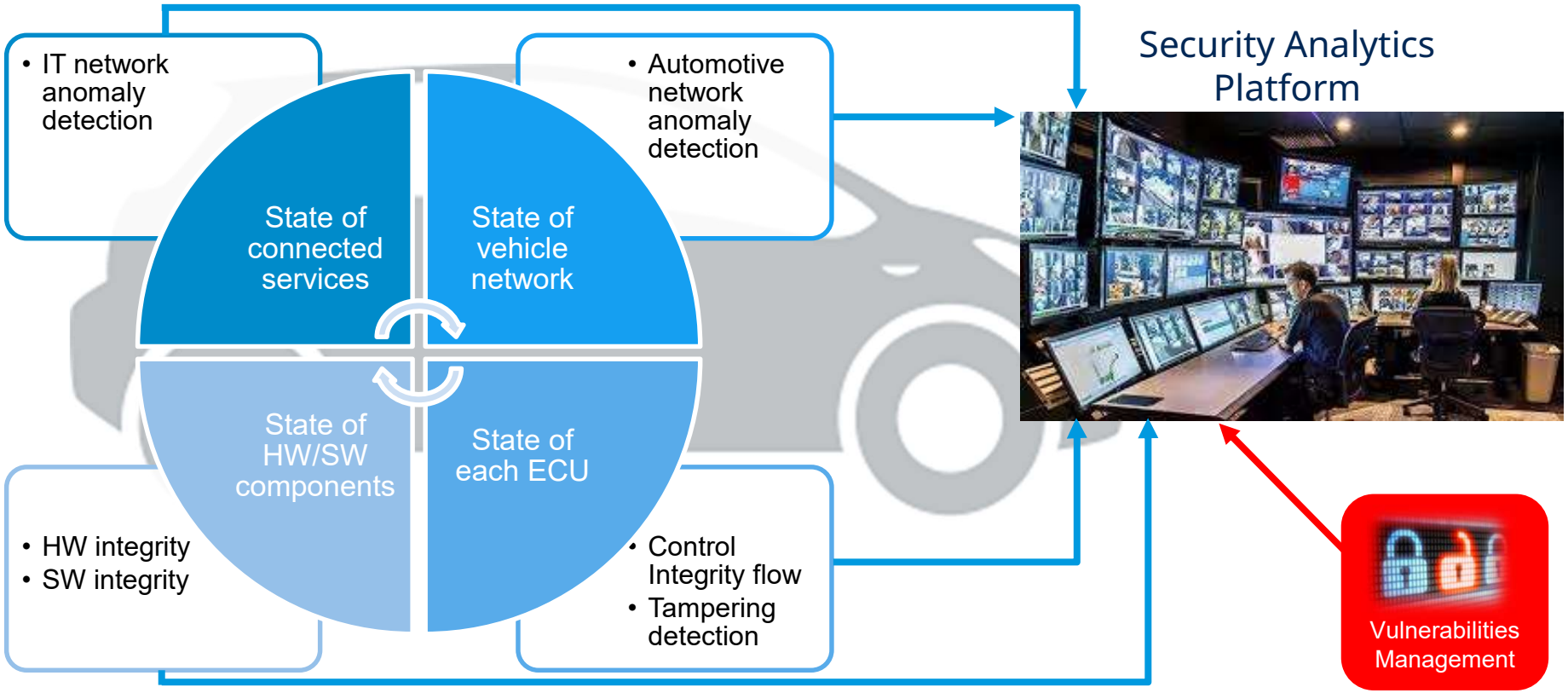


Vehicle Cyber Security state – WP.29 R155 Monitoring



Measurements of these states estimate vehicle state

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

Vulnerability

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

Exploit / Attack

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

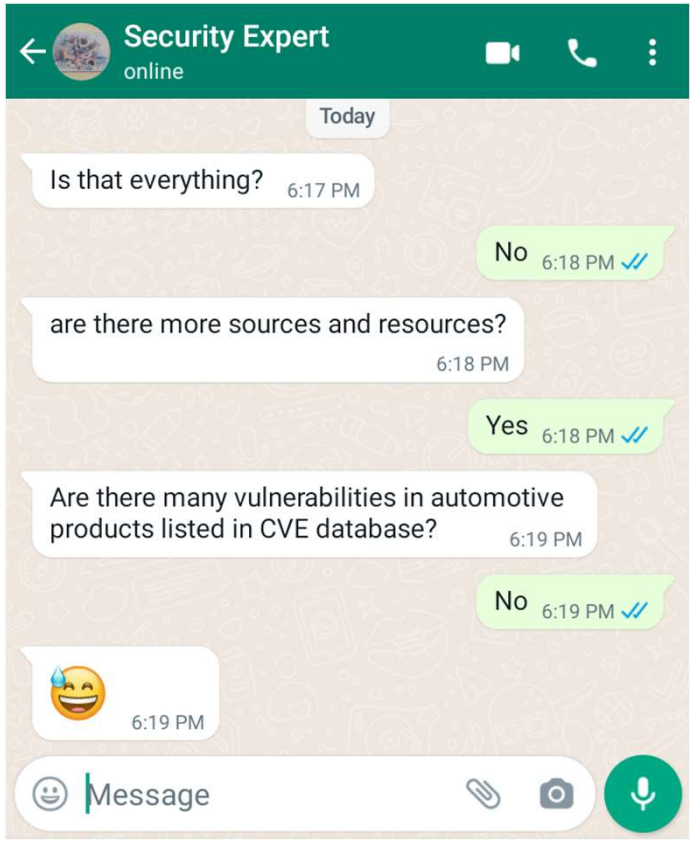
Common Weakness Enumeration: list of bad practices leading to vulnerable implementations https://cwe.mitre.org/

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

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')

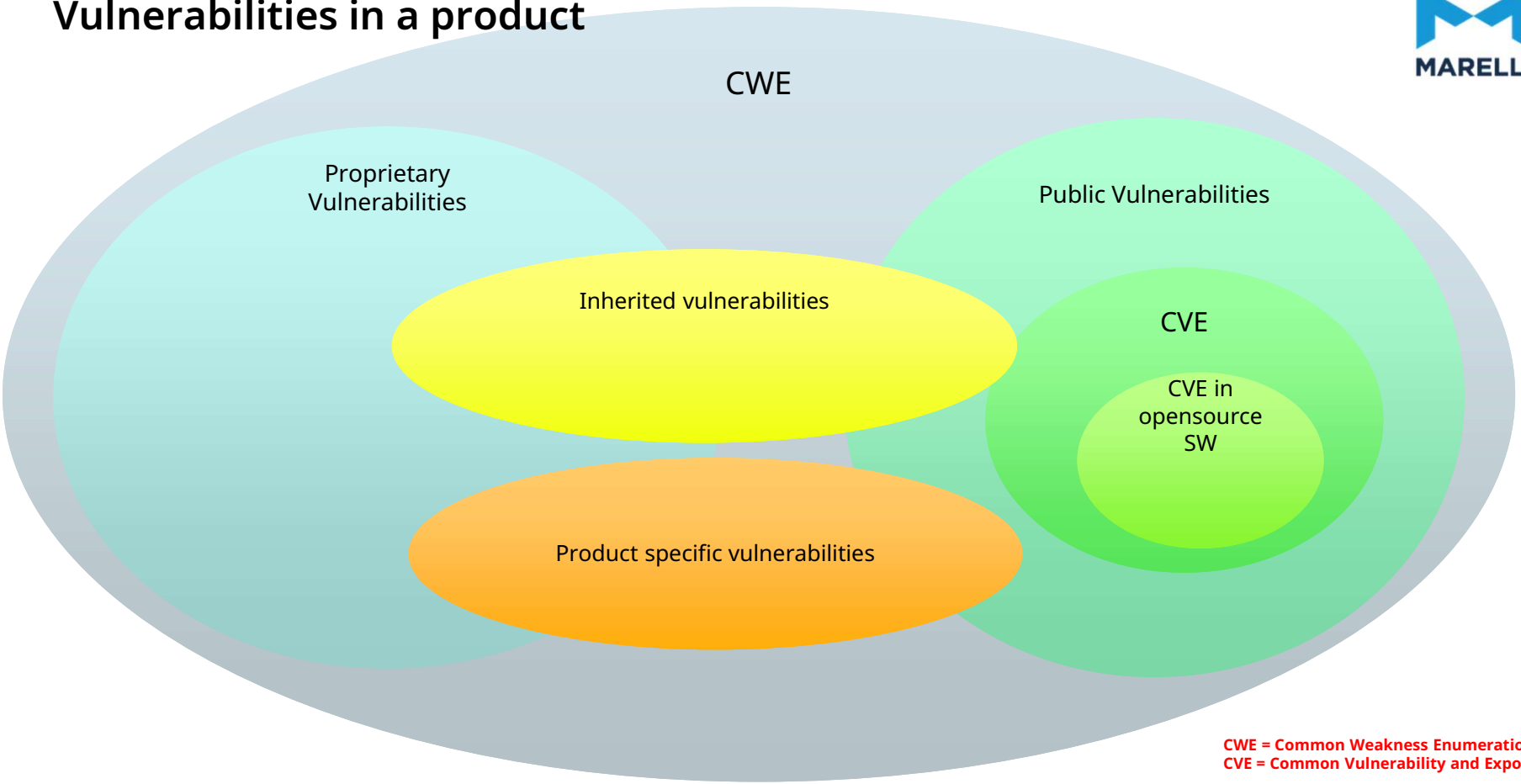
Vulnerability CVE-2017-1000251: Linux kernel versions from 3.3-rc1 contain a vulnerable implementation of L2CAP EFS within the BlueZ module.

Attack: take control of target Android device

Ref: *https://www.armis.com/blueborne/#/technical*

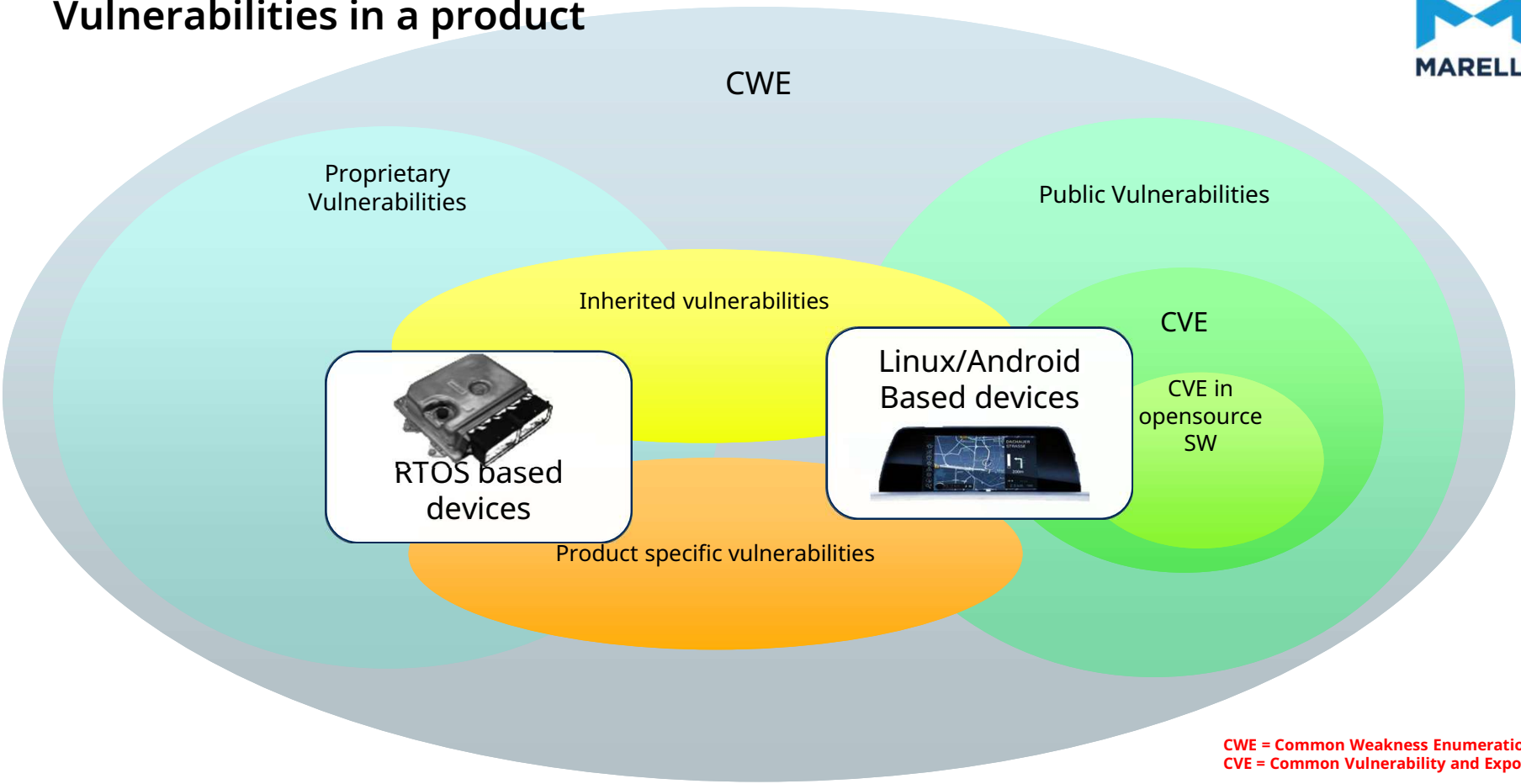
CWE = Common Weakness Enumeration
CVE = Common Vulnerability and Exposure

Vulnerabilities in a product



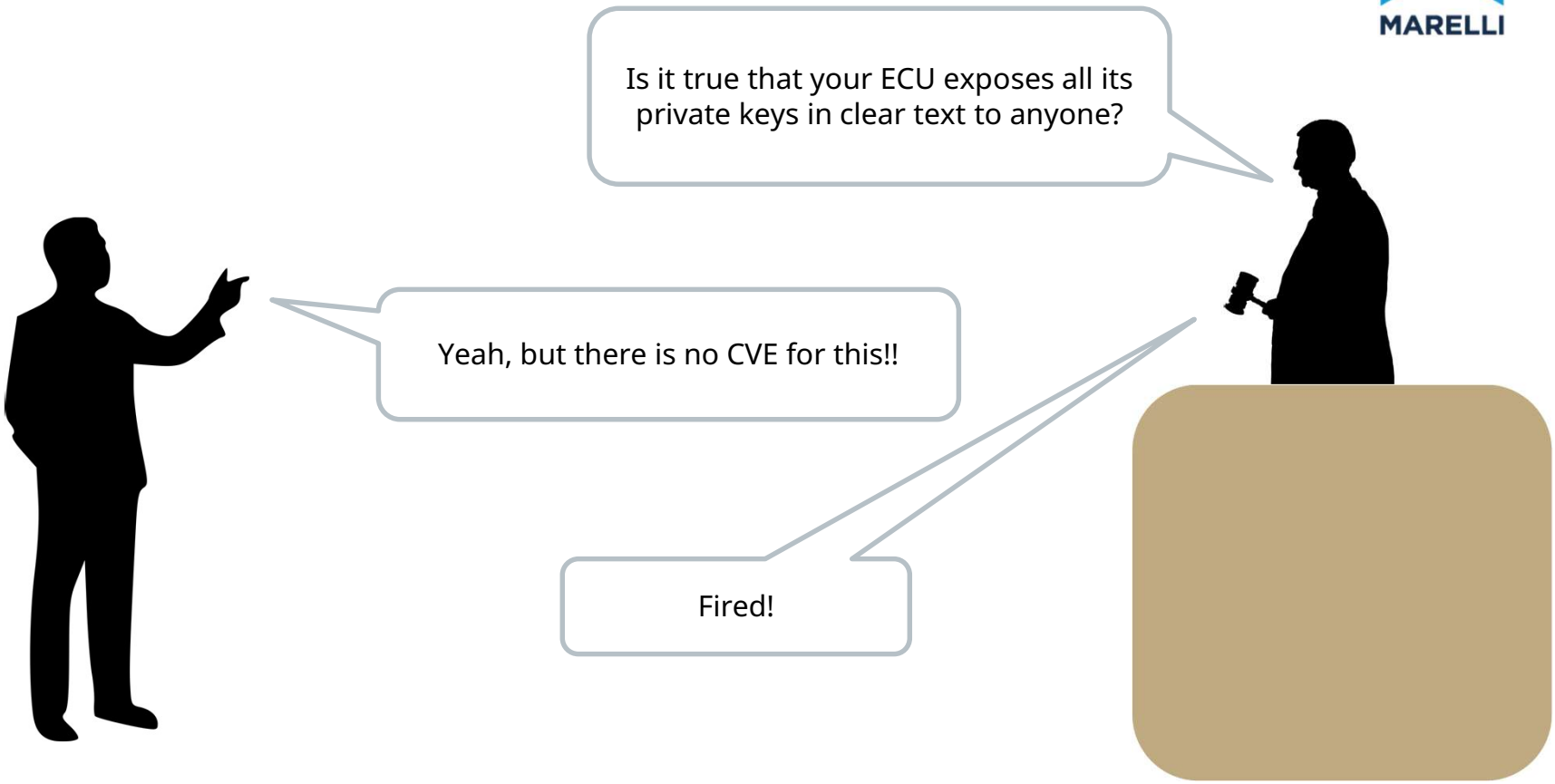
CWE = Common Weakness Enumeration
CVE = Common Vulnerability and Exposure

Vulnerabilities in a product

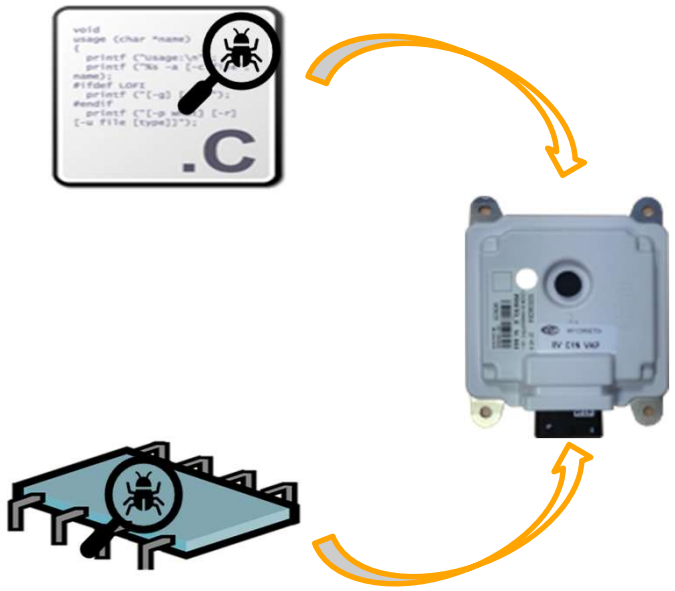


CWE = Common Weakness Enumeration
CVE = Common Vulnerability and Exposure

Is your definition of vulnerability vulnerable?



Inherited Vulnerabilities – Relations with suppliers



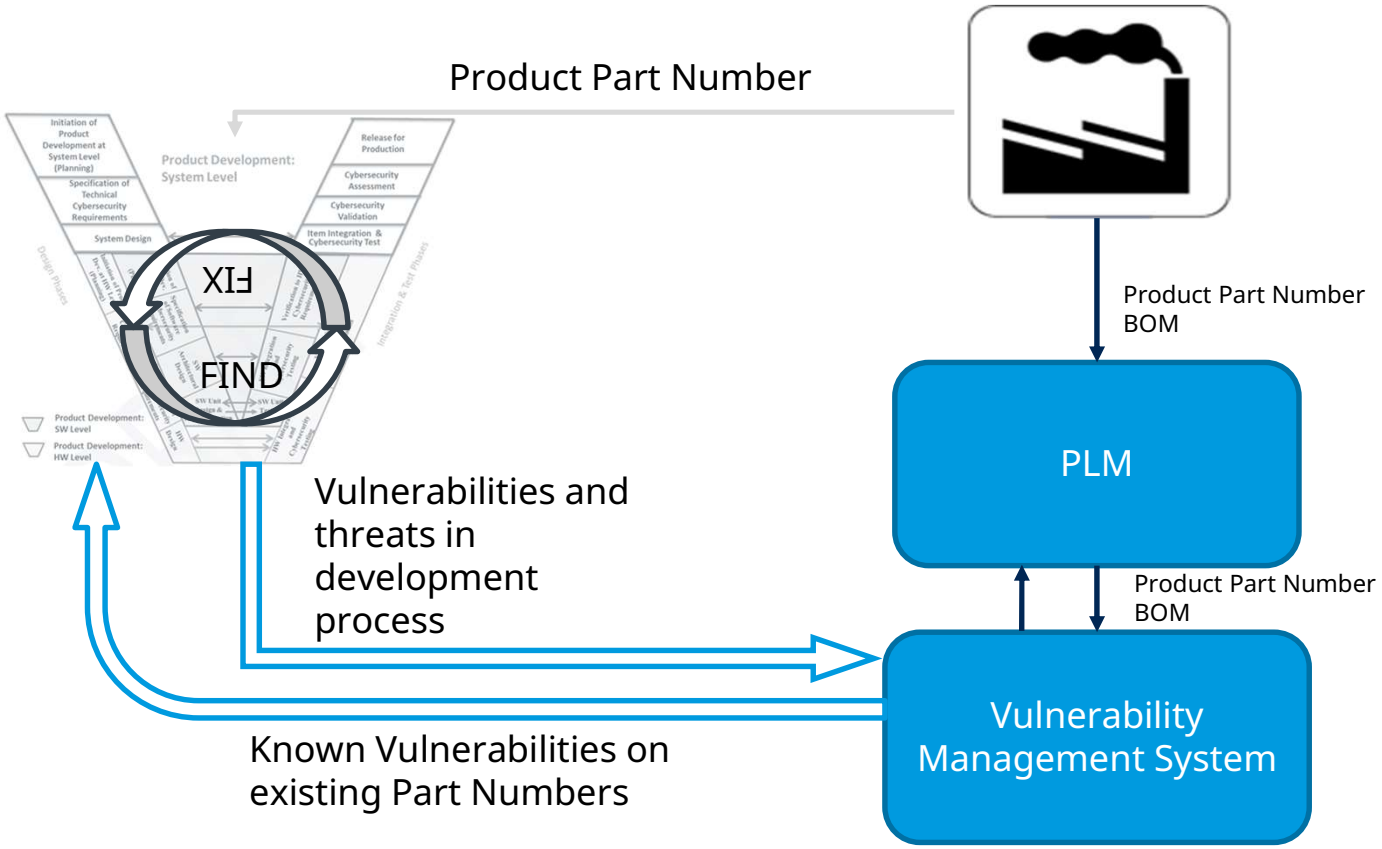
Most products integrate HW and SW components from third parties such as

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

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

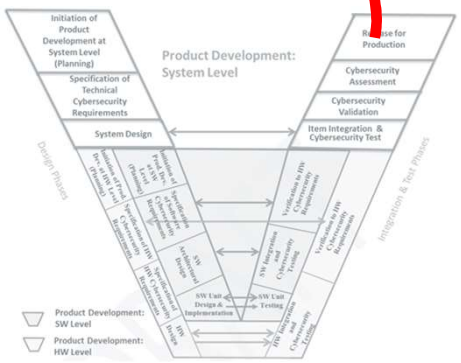
Vulnerabilities Management Workflows

Vulnerabilities Management – Product Development phase



PLM = Product Lifecycle Management

Vulnerabilities Management – Operation Phase



SW images

PLM

Product Part Number
BOM

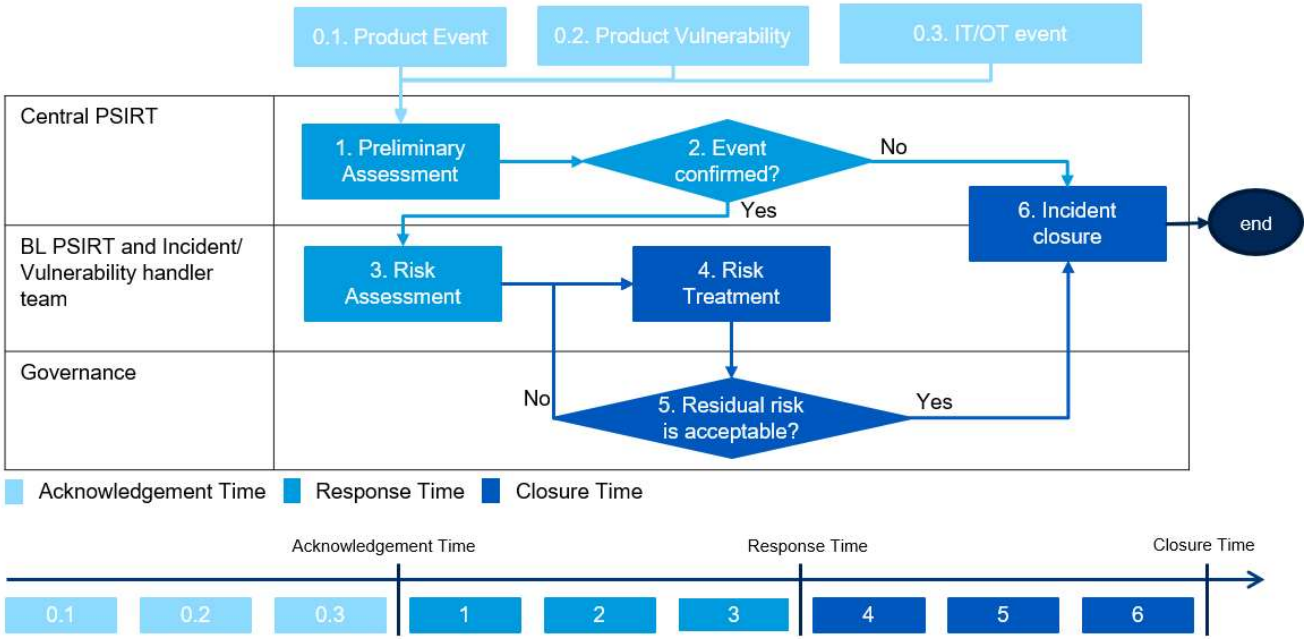
Vulnerabilities and threats on **production** SW images

Vulnerability Management System

Security Alert

Customer notification
3rd parties notification
...

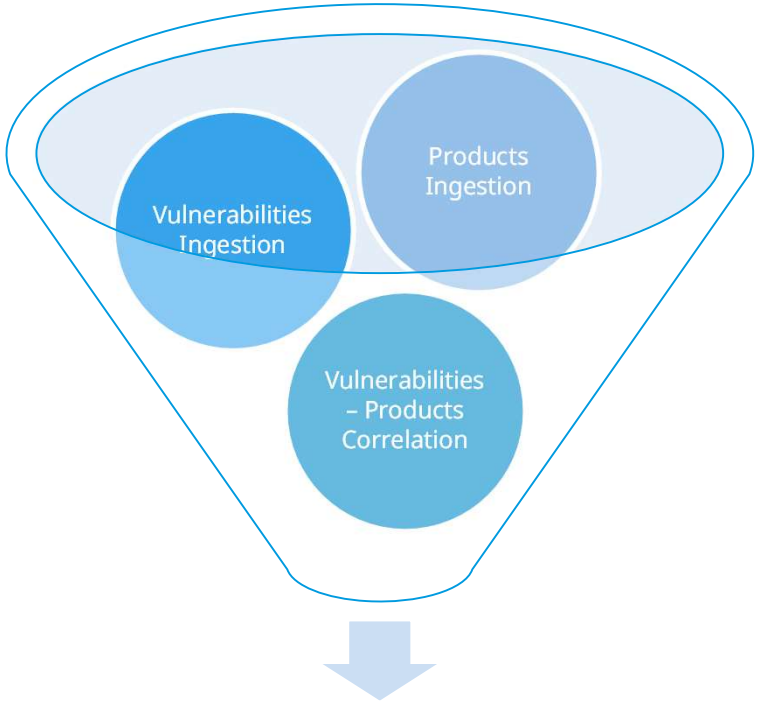
What is we manage a vulnerability as an incident?
PSIRT Workflows and key facts



- 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

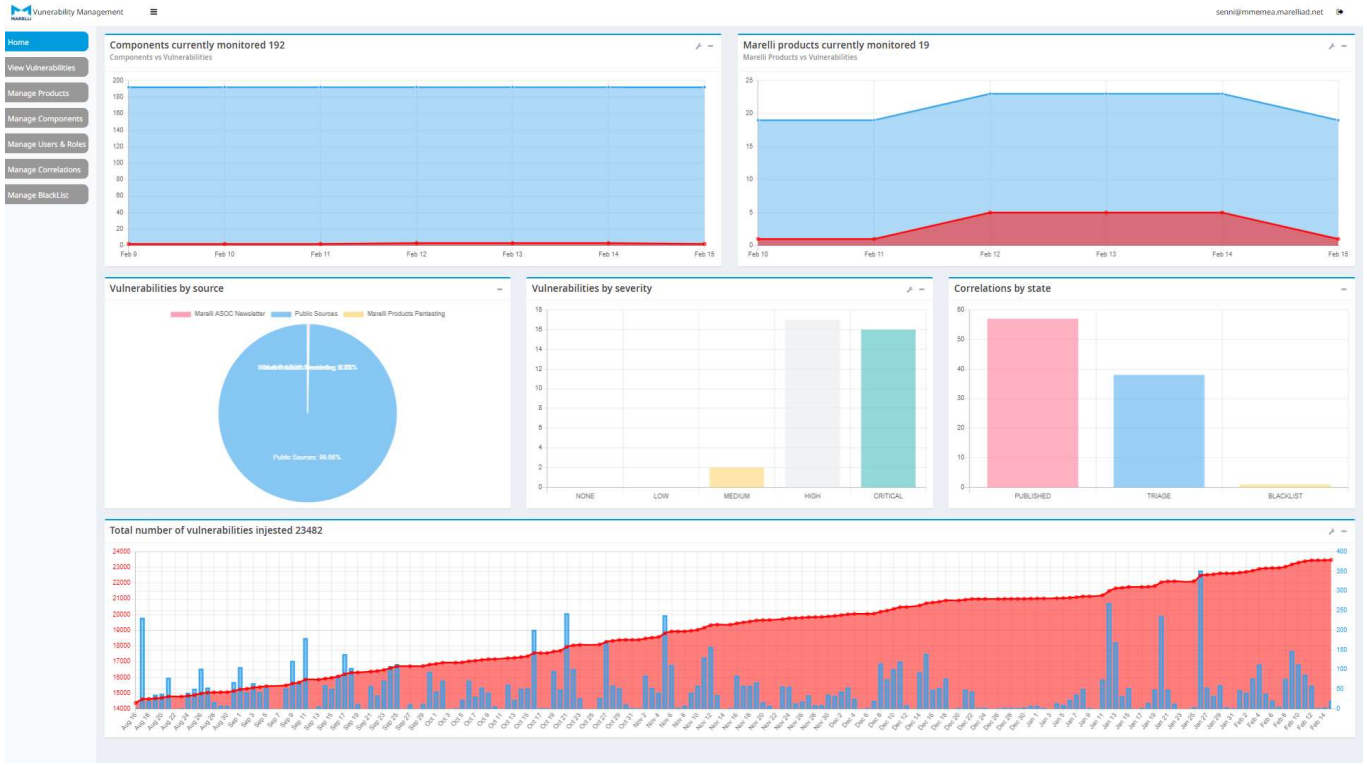


- **Vulnerabilities Ingestion:**
  - Public sources;
    - NVD
    - JVN
  - Auto-ISAC;
  - Proprietary sources (simplified list)
    - Specific car-tampering;
    - Findings of VARA and penetration tests run on products.
    - Suppliers
- Products ingestion:
  - Typically proprietary format stored in PLM system.

Products vulnerabilities management

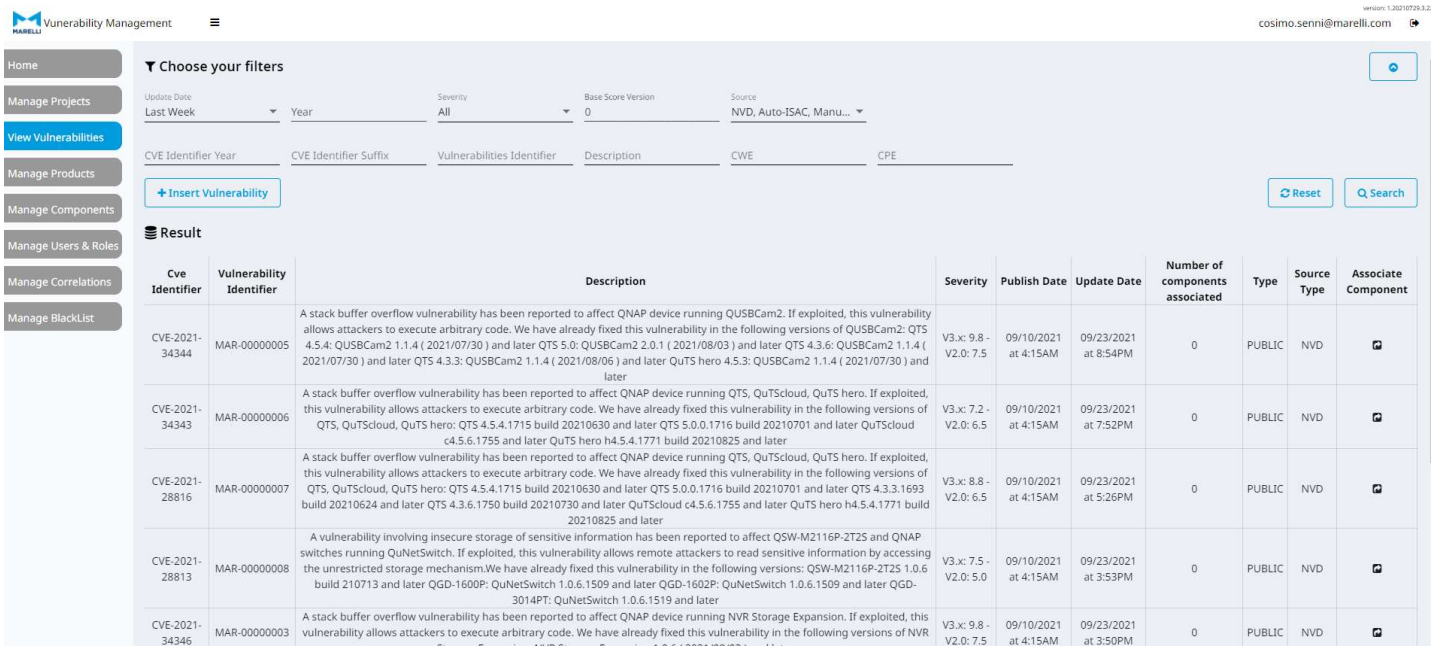
The center of all the system are products.

Vulnerability Management System for Products



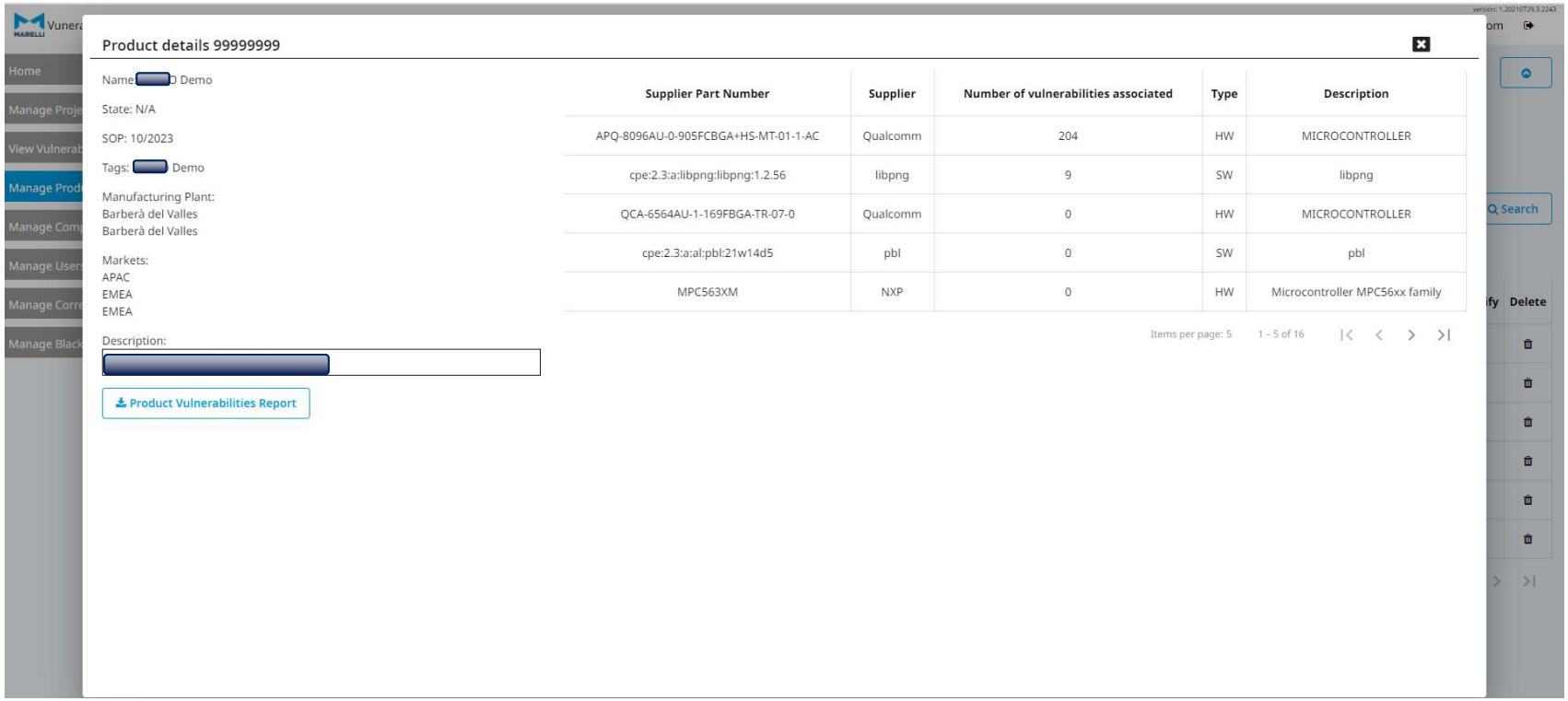
Vulnerability Management System for Products
Vulnerabilities DB

Vulnerabilites page



Vulnerability Management System for Products
Products page

Vulnerability Management System for Products
Product Detail and vulnerabilities



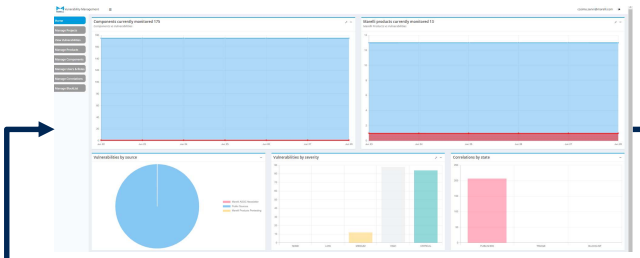
Marelli Vulnerability Management Platform – Supported Use Cases

- 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

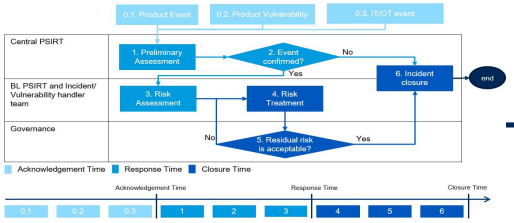
Vulnerabilities on Marelli products are managed as standard incidents.

Integration between Marelli Vulnerability Management Platform is planned as described below



Marelli Vulnerability Management Platform

New Vulnerability discovered in a product



Marelli PSIRT

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