Decommissioning Report

Revision

Version 5
1/19/22 8:12 AM

SME

Charles Wilson

Abstract

This document describes the process used to create the decommissioning report.

Group / Owner

DevOps / Information Systems Security Developer

Motivation

This document is motivated by the need to have formal processes in place for managing and reporting on the decommissioning of deployed safety-critical, cyber-physical systems for certification of compliance to standards such as **ISO 21434** and **ISO 26262**.

License

Overview

Decommissioning of vehicles comes in two forms:

- RMA (Return Merchandise Authorization) [1]
- EoL (End-of-Life)

Although both cases entail taking the vehicle out of the field, each requires unique security activities. When it is necessary to return a component for failure analysis, there is a need to maintain as much of the relevant state as possible. This poses many issues as the relevant information may be entangled with other security-relevant information which we desire not to expose. Things are less complicated when the desire is to permanently remove a vehicle from service as it is far easier to scrub a system entirely [3] than selectively remove sensitive information.

Both cases are discussed in detail in the **Decommissioning Plan** [2] created during the foundation phase.

Reports

Non-RMA-necessary Asset Removal Report

The **non-RMA-necessary Asset Removal Report** details the security-relevant elements removed and associated activities performed in order to make a component ready for return to supplier for repair.

The report should be organized into summary and details sections. The summary includes:

- Name of the component
- Description of the component
- Component SKU
- Component serial number
- Image of the component

The details section contains one or more activities. Each of these is organized into summary and activity step sections. The summary includes:

- activity title (unique)
- security-relevant element impacted
- Description of the activity's scope

Individual activities steps include:

- Activity step number (unique)
- Security-relevant element impacted
- Action taken
- Verification step

It is recommended that the report be generated from a portable data representation so that it can be programmatically manipulated.

Cybersecurity Decommissioning Report

The **Cybersecurity Decommissioning Report** details the security-relevant elements removed and associated activities performed in order to make a component ready for disposal.

The report should be organized into summary and details sections. The summary includes:

- Name of the component
- Description of the component
- Component SKU
- Component serial number
- Image of the component
- List of all security-relevant elements (used to cross-check activity list)
- Description of disposal mechanism

The details section contains one or more activities. Each of these is organized into summary and activity steps sections. The summary includes:

- activity title (unique)
- security-relevant element impacted
- Description of the activity's scope

Individual activity steps include:

- Activity step number (unique)
- Security-relevant element impacted
- Action taken
- Verification step

It is recommended that the report be generated from a portable data representation so that it can be programmatically manipulated.

References

1. **Return merchandise authorization**
   https://en.wikipedia.org/wiki/Return_merchandise_authorization
2. **Decommissioning Plan** (AVCDL secondary document)
3. **NIST SP 800-88 r1 – Guidelines for Media Sanitization**
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf