#

CIP Release Security Checklist

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2022-01-06	Initial draft	Yasin User	To be reviewed by CIP Security WG members

---

---

1. Objective

The primary objective of this document is to provide a list of security items to check before each release.

2. Scope

Scope of this document is to meet IEC-62443-4-1 SM-11 (Assessing and addressing security-related issues) and SM-12 (Process verifications) security requirements.

3. Checklist Usage

Before a CIP version can be released, each of those items has to be checked. If an item cannot be checked, it must be mentioned in the release notes including at least: - Item which was not checked - Reason for not checking it (e.g. no official fix is available yet, fix will be included in next release, ...) - Potential impact for the CIP users Any other helpful information should be included. This exemption is not useable if the security issue was not already included in the last release, as a new release should never introduce new known security issues.

4. Checklist

- Have all security-related issues been addressed and tracked to closure?
  - Check Kernel and Core WG issue tracker.
  - Check the upstream CVE list.
- Have the following processes been completed, including some documentation?
  - The threat model was reviewed in the last year.
  - The process of reviewing security related issues has been reviewed in the last year.
  - The secure design best practices were reviewed in the last year.
  - The secure coding standards were reviewed in the last year.
  - Were the static code analysis results checked and issues created if needed?
  - Were the test results checked and issues created if needed?
- Are all to be released files signed?

TODO: include items for development and testing when processes are completed.