

# [2017-11-08] Change Log

- [New version of CQM \(v1.2.12\) and Kiuwan Engine](#)
  - [New Security Rules](#)
    - [HTML](#)
    - [Java](#)
    - [JSP](#)
  - [Improvements in Kiuwan Engine \(master.p461.q7422.a1731\)](#)

## New version of CQM (v1.2.12) and Kiuwan Engine



A new Kiuwan's CQM version (v.1.2.12) is available.

Basically, v1.2.12 contains **new Security rules for HTML, Java and JSP**.

- If you are using *CQM*, these new rules are active and will be applied to new analyses.
- If you are using your own *custom model*, you can activate them in case you want to be applied to your code.

**In order for these new rules be applicable, your Kiuwan account must allow for automatic engine upgrade.** Unless you have blocked Kiuwan Engine, Kiuwan Local Analyzer will automatically upgrade it to the last version once a new analysis is run.

You can find new rules by comparing v1.2.12 of CQM against previous version. A detailed description of the behavior of these new rules is available in rule's description.

## New Security Rules

Support to Security has been improved with the **addition of new rules** as well as **continuous improvements in security rules execution**.

### HTML

- Password input field is not masked (CWE:549)

### Java

- Avoid using an user controlled Primary Key into a query (CWE:566)
- Plaintext Storage of a Password (CWE:256)
- Array index coming from a non neutralized vulnerable input (CWE:129)
- Not using a Random IV with CBC Mode (CWE:329)
- Hardcoded cryptographic keys (CWE:321)
- Avoid sensitive information exposure through error messages (CWE:209)
- Execution After Redirect (EAR) (CWE:698)
- NULL Pointer Dereference (CWE:476)

### JSP

- Unprotected transport of credentials (CWE:523)
- Information exposure through strings sent by GET (CWE:598)
- Password input field is not masked (CWE:549)

## Improvements in Kiuwan Engine (master.p461.q7422.a1731)

New Kiuwan engine contains enhanced versions of parsers and rules:

- Complete grammar support for **Cobol AcuCOBOL-GT** (MicroFocus subdialect)
- Enhancements in *parsers*: ABAP and PL-SQL
- Bug fixing, performance and reliability issues in Security rules for Java and JSP *rules*