[2020-09-15] Change Log

Contents:

Angular dynamic components

We have expanded our JavaScript support. This release allows you to check for dynamic components that were built in an Angular Framework.

The underlying vulnerability from using dynamic components construction is not different from other "eval injection" issues, review the following links for more information:

- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection').
- Client-side template injection

JSX React

Also, in our JavaScript support, we had partial support for React. Now, this support is extended with JSX technology.

JSX, or JavaScript XML, is an XML-like syntax extension to ECMAScript part of the React library. The complete specification can be checked at Draft: JSX Specification.

The following elements have been identified as potential security flaws and detected by the existing JS rules:

1. dangerouslySetInnerHTML attribute acts as the entrance door to perform an XSS attack (See dangerouslySetInnerHTML).
2. Server-side rendering attacker-controlled initial state XSS in React apps using Redux.
3. XSS in explicit calls to React.createElement(...) with untrusted props or children (See Avoiding XSS in React is Still Hard).
4. Attribute injection also leads to XSS.

In React, the HTML code is embedded into the JS code, so the HTML code must be checked to mark sources, sinks, or neutralization (For example: <input> elements).

Also, the embedded HTML code is analyzed by Kiuwan with the rules from the HTML technology. The following existing checks might be applied:

OPT.HTML.AutocompleteOnForSensitiveFields.

OPT.HTML.MissingPasswordFieldMasking.

OPT.HTML.TargetBlankVulnerability.

OPT.HTML.SandboxAllowScriptsAndSameOrigin.

OPT.HTML.SpecifyIntegrityAttribute.

Jenkins Kiuwan plugin update

Kiuwan has its plugin to integrate with a Jenkins environment:

- Jenkins Plugin
- jenkinsci/kiuwan-plugin

This new version includes the following updates:

- Connection Profiles: Currently, Kiuwan Jenkins Plugin connection settings are limited to one configuration per Jenkins installation. Now, you can set several profiles, you can use multiple accounts, and Kiuwan On-Premises customers may use different environments.
- New analysis result dashboard.
- Improve support for short-lived nodes.
- Pipeline support.

Other bug fixes and improvements

- **SAS-5238** (REST API) new endpoint to retrieve ‘last delivery’ analysis results
- **SAS-5235** Code Security. PDF and CSV reports don’t match the exported vulnerabilities
- **SAS-5211** Typo in PDF vulnerabilities report
- **SAS-5208** (REST API) Python sample code for Rest API client does not work

- **SAS-5181** Use class attributes with user data in singleton beans
- **SAS-5141** QMM does not export rules custom configuration
- **SAS-5071** (REST API) add additional info at GET /applications endpoint
- **SAS-4955** Rules compare is not working as expected: missing modified rules
- **SAS-4902** mute defect - default option + rest api
- **SAS-4843** Missing field "Remediation" in the CSV export for a rule
- **SAS-4836** (REST API) Add ‘unparsed files’ to responses to any ‘analysis’ related endpoint
- **SAS-4817** Group by portfolio option in CS/CA dashboard is not excluding deliveries
- **SAS-4747** disabled the ‘reset password’ option for disabled users
- **SAS-4738** disable the kiuwan account removal

- **QAK-6475** PARSE ERROR javascript file
- **QAK-6467** Projects is constantly running into an timeout
- **QAK-6466** FP in OPT.JAVASCRIPT.PropertyNamesUniqueness on "async"
- **QAK-6443** ERROR analyzing C application with newest engine
- **QAK-6439** BUG C++ Java returned 1: java.lang.StackOverflowError
- **QAK-6432** PARSE ERROR para fichero 4GL
- **QAK-6424** FP OPT.JAVA.FMETODOS.GNE
- **QAK-6413** Javascript parsing error