This advisory discloses security vulnerabilities found and fixed in Comala Workflows. We recommend upgrading Comala Workflows to the latest supported version for your release of Confluence.

Affected Versions

These vulnerabilities affect all versions of Comala Workflows up to and including 4.6.1. The following versions have been released containing fixes for the issues mentioned below:

Comala Workflows 4.6.2 for Confluence 5.4+
Comala Workflows 4.5.4 for Confluence 4.3+

XSS Vulnerabilities

Severity

Comalatech rates the severity of these issues as High according to the published Atlassian Security Levels.

This is an independent assessment and you should evaluate its applicability to your own IT environment.

Description

We have fixed several reflective and stored cross site scripting vulnerabilities in Comala Workflows. In all cases the attacker needs to have an active account on the Confluence server.

Specific areas that have been fixed

- Task name display is several reports
- Legacy attachment and embed macros
- Several fields on workflow designer

Risk Mitigation

We recommend you upgrade Comala Workflows to 4.6.2 or 4.5.4.

If upgrading is not immediately possible, you can limit the number of users that have the ability to exploit these vulnerabilities.

- Disable the legacy attachment and embed macros.
- Disable page workflows to prevent adhoc task creation.
- Edit workflows to prevent tasks being created (taskable parameter on states)

Fix

Upgrade Comala Workflows to the latest supported version for your Confluence instance

Comala Workflows 4.6.2 for Confluence 5.4+
Comala Workflows 4.5.4 for Confluence 4.3+

XSRF Vulnerabilities

Severity

Comalatech rates the severity of these issues as Medium according to the published Atlassian Security Levels.

This is an independent assessment and you should evaluate its applicability to your own IT environment.

Description
We have updated several actions within the Comala Workflows plugin to prevent cross site request forgery (XSRF) vulnerabilities. These XSRF vulnerabilities could allow an attacker to trick users into unintentionally modifying workflow settings or approving pages if they have specific knowledge about the Confluence setup.

**Risk Mitigation**

We recommend you upgrade Comala Workflows to 4.6.2 or 4.5.4.

**Fix**

Upgrade Comala Workflows to the latest supported version for your Confluence instance

Comala Workflows 4.6.2 for Confluence 5.4+

Comala Workflows 4.5.4 for Confluence 4.3+

**Acknowledgements**

The Comalatech team thanks Julian Krautwald (discovery, analysis) from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues and working with us as we addressed them.