

# Security Advisory 2020-04-29 - Blind SQL Injection on the Audit Log and RCE on Post Functions and Scheduled Reports

## Xporter for Jira Server and Data Center - Blind SQL Injection on the Audit Log

Summary	Blind SQL Injection on the Audit Log
Advisory Release Date	29 Apr 2020 10:00 AM CET
Product	Xporter for Jira Server & Data Center Xporter for Jira Cloud customers are not affected.
Affected on Xporter for Jira Server & Jira Data Center Versions	<ul style="list-style-type: none"><li>From 5.7.0 to 6.2.4</li></ul>
Fixed on Xporter Jira Server & Jira Data Center Versions	<ul style="list-style-type: none"><li>6.3.0</li></ul>

### Summary of Vulnerability

This advisory discloses a **critical severity** security vulnerability that was present in Xporter for Jira Server & Data Center. Versions of Jira Server & Data Center affected by this vulnerability:

- from 5.7.0 to 6.2.4 (fixed in 6.3.0).

Customers who have upgraded Xporter for Jira Server & Data Center to version 6.3.0 or higher are not affected.

Customers who are on any of the affected versions, upgrade your Xporter for Jira Server & Data Center installations immediately to fix this vulnerability.

### Severity


We rate the severity level of this vulnerability as **critical**, according to the scale published in [Atlassian severity levels](#). The scale allows us to rank the severity as critical, high, moderate or low.

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

### Description

We detected Blind SQL Injection vulnerabilities on the Audit Log.

This issues can be tracked here:

-  [XPORTE-2958](#) - Blind SQL injection at Audit Log CLOSED

### Fix

We have released Xporter for Jira Server & DC version 6.3.0 which is available for upgrade through the Atlassian Marketplace.

## Xporter for Jira Server and Data Center - RCE on Post Functions and Scheduled Reports

Summary	RCE on Post Functions and Schedule Reports
---------	--

<b>Advisory Release Date</b>	10 Apr 2020 10:00 AM CET
<b>Product</b>	Xporter for Jira Server & Data Center Xporter for Jira Cloud customers are not affected.
<b>Affected on Xporter for Jira Server &amp; Jira Data Center Versions</b>	<ul style="list-style-type: none"> <li>From 5.0.0 to 6.2.4</li> </ul>
<b>Fixed on Xporter Jira Server &amp; Jira Data Center Versions</b>	<ul style="list-style-type: none"> <li>6.3.4</li> </ul>

## Summary of Vulnerability

This advisory discloses a **critical severity** security vulnerability that was present in Xporter for Jira Server & Data Center. Versions of Jira Server & Data Center affected by this vulnerability:

- from 5.0.0 to 6.2.4 (fixed in 6.3.4).

**Customers who have upgraded Xporter for Jira Server & Data Center to version 6.3.4 or higher are not affected.**

**Customers who are on any of the affected versions, upgrade your Xporter for Jira Server & Data Center installations immediately to fix this vulnerability.**

## Severity



We rate the severity level of this vulnerability as **critical**, according to the scale published in [Atlassian severity levels](#). The scale allows us to rank the severity as critical, high, moderate or low.

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

## Description

We detected RCE vulnerabilities on the Multi-action Workflow Post Function and Scheduled Reports. An attacker could create a template with malicious code and change the output file extension before creating the Post Function or Scheduled Report.

This issues can be tracked here:

-  [XPORTR-3457](#) - RCE vulnerability at Multi-action Workflow Post Function CLOSED
-  [XPORTR-2959](#) - RCE vulnerability at Scheduled Report CLOSED

## Fix

We have released Xporter for Jira Server & DC version 6.3.4 which is available for upgrade through the Atlassian Marketplace.

## What You Need to Do

### Upgrade

You can upgrade to the latest version of Xporter for Jira Server & Data Center using the Universal Plugin Manager as explained in [Updating apps](#).

### Support

If you have questions or concerns regarding this advisory, please raise a support request at <https://xportersupport.xpand-it.com>.