

# Security Advisory - July, 2021



We recommend the update of Xray for Jira Server & Data Center to the 4.3.6 - latest version.

## Xray for Jira Server and Data Center - Remote Code Execution on Document Generator Export

Summary	Remote Code Execution on Document Generator Export
Advisory Release Date	21 Jul 2021 10:00 AM CET
Product	Xray for Jira Server & Data Center
Affected on versions	<ul style="list-style-type: none"><li>4.1.0 to 4.3.2</li></ul>
Fixed on versions	<ul style="list-style-type: none"><li>4.3.3 and later</li></ul>

### Summary of Vulnerability

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

- 4.1.0 to 4.3.2 (fixed in 4.3.3 and later).

**Customers who have upgraded Xray for Jira Server & Data Center to version 4.3.3 or higher are not affected.**

**Customers who are on any of the affected versions, upgrade your Xray 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 [Bugcrowd's Vulnerability Rating Taxonomy](#). 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 Remote Code Execution vulnerabilities on the Document Generator Export feature.

These issues can be tracked here:

 [XRAY-7694](#) - Remote Code Execution - Document Generator Export CLOSED

### Fix

We have released Xray for Jira Server & Data Center version 4.3.3 which is available for upgrade through the Atlassian Marketplace.

## What You Need to Do

### Upgrade

You can upgrade to the latest version of Xray 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 [here](#).