

Security Advisory - March, 2022



We recommend the update of Xray Test Management for Jira Server & Data Center to the [6.1.2.1](#) - latest version.

Xray Test Management for Jira Server and Data Center - Remote Code Execution on Document Generator

Summary	Remote Code Execution on Document Generator
Advisory Release Date	22 Mar 2022 10:00 AM CET
Product	Xray Test Management for Jira Server & Data Center
Affected on Xray Test Management for Jira Server & Jira Data Center Versions	<ul style="list-style-type: none">6.1.2 and earlier
Fixed on Xray Test Management Jira Server & Jira Data Center Versions	<ul style="list-style-type: none">6.1.2.1 and later

Summary of Vulnerability

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

- 6.1.2 and earlier (fixed in 6.1.2.1 and later).

Customers who have upgraded Xray Test Management for Jira Server & Data Center to version 6.1.2.1 or higher are not affected.

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

Severity

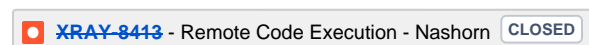
We rate the severity level of these vulnerabilities as **critical**, according to the scale published in [Bugcrowd's Vulnerability Rating Taxonomy](#). The scale allows us to rank the severity as critical, high, moderate, or low.

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

Description

We detected a Remote Code Execution vulnerability on the Document Generator.

The issue can be tracked here:



Fix

We have released Xray for Jira Server & DC version [6.1.2.1](#) 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](#).