

# Security Advisory 2020-04-24 - Xray for Jira Server and Data Center

## Xray for Jira Server and Data Center - XXE vulnerability at XML result import

Summary	XXE vulnerability at result import (Test Run Result field)
Advisory Release Date	10 Apr 2020 10:00 AM CET
Product	Xray for Jira Server & Data Center Xray for Jira Cloud customers are not affected.
Affected on Xray for Jira Server & Jira Data Center Versions	<ul style="list-style-type: none"><li>All versions from 2.1.0 up to 3.6.2</li></ul>
Fixed on Xray Jira Server & Jira Data Center Versions	<ul style="list-style-type: none"><li>3.6.3</li></ul>

### Summary of Vulnerability

This advisory discloses a **critical severity** security vulnerability which was present Xray versions of for Jira Server & Data Center from [2.1.0](#) until [3.6.3](#). Versions of Jira Server & Data Center affected by this vulnerability:

- from 2.1.0 to 3.6.2 (fixed in 3.6.3).

**Customers who have upgraded Xray for Jira Server & Data Center to version 3.6.3 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.**

## XXE vulnerability at XML result import (Test Run Result field)

### 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.

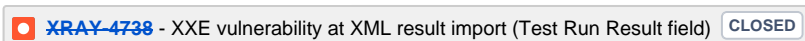
This is our assessment and you should evaluate its applicability to your own IT environment.

### Description

There is an XXE vulnerability while using POST method of **any** of the *import/execution/\* XML* endpoints which allows attackers to get read access to the filesystem on behalf of the user running Jira.

Attackers are able to access filesystem by uploading a specific XML as result in any of the Xray endpoints accepting XML result files.

This issue can be tracked here:



### Fix

We have released Xray for Jira Server & DC version 3.6.3 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](#).

### Mitigation

#### Workaround 1 - Tomcat (*requires restart*)

Block the endpoint from being accessed directly in the Tomcat configuration files, only for the POST method:

1. Shut down the application, and backup your `$application-install/atlassian-jira/WEB-INF/web.xml` file
2. Add the following block inside the `<web-app>` element:

```
<security-constraint>
  <web-resource-collection>
    <url-pattern>/rest/raven/1.0/import/execution/junit/*</url-pattern>
    <url-pattern>/rest/raven/1.0/import/execution/testng/*</url-pattern>
    <url-pattern>/rest/raven/1.0/import/execution/nunit/*</url-pattern>
    <url-pattern>/rest/raven/1.0/import/execution/robot/*</url-pattern>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint />
</security-constraint>
```

3. Restart the Jira application
4. If you try to send a POST request to the endpoint `<JIRA_BASE_URL>/rest/raven/1.0/import/execution` that accepts XML file format a 403 error with Jira HTML page stating that "Access to the requested resource has been denied" will be returned

## Workaround 2 - Reverse Proxy

Block the endpoint from being accessed on the proxy server-side, only for the POST method (Tested on Apache HTTPD):

1. Open the virtual host configuration
2. Add the following inside the virtual host to block the endpoint POST actions `/rest/raven/1.0/import/execution/(junit|testng|nunit|robot)`

```
<LocationMatch "/rest/raven/1.0/import/execution/(junit|testng|nunit|robot)">
  Deny from all
</LocationMatch>
```

3. Ensure all connectors pass through the proxy
4. Restart Apache

### Example Virtual Host:

```
<VirtualHost *:80>

    ServerName getxray.app

    ProxyRequests Off
    ProxyVia Off

    <Proxy *>
        Require all granted
    </Proxy>

    <LocationMatch "/rest/raven/1.0/import/execution/(junit|testng|nunit|robot)">
        Deny from all
    </LocationMatch>

    ProxyPass          /jira          http://localhost:8080/jira
    ProxyPassReverse    /jira          http://localhost:8080/jira

</VirtualHost>
```

## Support

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