Security Advisory - July, 2021

⚠ We recommend the update of Xporter for Jira Server & Data Center to the 6.7.5 - latest version.

Xporter for Jira Server and Data Center - SQL Injection on Process Manager and Audit Log

Summary	SQL Injection on the Process Manager and Audit Log
Advisory Release Date	21 Jul 2021 10:00 AM CET
Product	Xporter for Jira Server & Data Center
Affected on Xporter for Jira Server & Jira Data Center Versions	• 6.7.1 and earlier
Fixed on Xporter Jira Server & Jira Data Center Versions	• 6.7.2 and later

Summary of Vulnerability

This advisory discloses security vulnerabilities classified as **critical** that were present in Xporter for Jira Server & Data Center.

Versions of Jira Server & Data Center affected by this vulnerability:

- 6.7.1 and earlier (fixed in 6.7.2 and later).

Customers who have upgraded Xporter for Jira Server & Data Center to version 6.7.2 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 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 SQL Injection vulnerabilities on the Audit Log and Process Manager features.

These issues can be tracked here:

~~XPORTER-3730~~ - SQL Injection - Administration Audit Log CLOSED

~~XPORTER-3731~~ - SQL Injection - My Exports CLOSED

~~XPORTER-3732~~ - SQL Injection - Administration Process Manager CLOSED

Fix

We have released Xporter for Jira Server & DC version 6.7.2 which is available for upgrade through the Atlassian Marketplace.

Xporter for Jira Server and Data Center - Local File Disclosure on Templates Management

Summary	Local File Disclosure on Templates Management
Advisory Release Date	12 Jul 2021 10:00 AM CET
Product	Xporter for Jira Server & Data Center
Affected on Xporter for Jira Server & Jira Data Center Versions	• 6.7.1 and earlier
Fixed on Xporter Jira Server & Jira Data Center Versions	• 6.7.2 and later

Summary of Vulnerability

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

- 6.7.1 and earlier (fixed in 6.7.2 and later).

Customers who have upgraded Xporter for Jira Server & Data Center to version 6.7.2 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 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 Local File Disclosure vulnerability on the Templates management.

This issue can be tracked here:

~~XPORTER-3733~~ - Local File Disclosure - Template file CLOSED

Fix

We have released Xporter for Jira Server & DC version 6.7.2 which is available for upgrade through the Atlassian Marketplace.

Xporter for Jira Server and Data Center - Remote Code Execution on Export/Import Settings and Templates export

Summary	Remote Code Execution on Export/Import Settings and Templates export
Advisory Release Date	12 Jul 2021 10:00 AM CET
Product	Xporter for Jira Server & Data Center
Affected on Xporter for Jira Server & Jira Data Center Versions	Export/Import Settings:

	• 6.7.1 and earlier Templates Export: • 6.7.2 and earlier
Fixed on Xporter Jira Server & Jira Data Center Versions	Export/Import Settings: • 6.7.2 and later Templates Export: • 6.7.3 and later

Summary of Vulnerability

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

- Export/Import Settings: 6.7.1 and earlier (fixed in 6.7.2 and later).
- Templates Export: 6.7.2 and earlier (fixed in 6.7.3 and later).

Customers who have upgraded Xporter for Jira Server & Data Center to version 6.7.3 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 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 Remote Code Execution vulnerabilities on the Export and Import Settings and Template Exports.

These issues can be tracked here:

~~XPORTER-3735~~ - Remote Code Execution - Export and Import Settings CLOSED

~~XPORTER-3776~~ - Remote Code Execution - Templates Export CLOSED

Fix

We have released Xporter for Jira Server & DC version 6.7.3 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 here.