

Sign In

Home > Advisories > Jaspersoft Security Advisory: August 05, 2026 - JasperReports Server - CVE-2026-16626



# Jaspersoft Security Advisory: August 05, 2026 - JasperReports Server - CVE-2026-16626

Share

Followers

## JasperReports Server: XXE Injection Vulnerability (Unauthenticated)

Original release date: August 05, 2026

Last revised: ---

CVE-2026-16626

Source: Jaspersoft

### Description

Unauthenticated XEE Injection vulnerability has been discovered in JasperReports Server.

Refer below for further details

### Product(s) Affected

- JasperReports Server versions 9.x
- JasperReports Server versions 10.x

### Summary

JasperReports Server is affected with the vulnerability mentioned below

| CVE-ID | Description | Impact |
|--------|-------------|--------|
|--------|-------------|--------|

|                |                                                                                                                                                                                             |                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-16626 | JasperReports Server contains vulnerabilities in its input validation and XML processing mechanisms that can be exploited by a remote unauthenticated attacker to bypass security controls. | A remote, unauthenticated attacker can exploit the vulnerability to bypass authentication controls and gain unauthorized access to protected application resources. |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

What Customers Should Do

Cloud Software Group strongly urges affected customers to install the relevant updated versions as soon as possible.

- **JasperReports Server v10.0.0:** Apply HF-10 - [hotfix\\_JRSP10.0.0\\_cumulative\\_20260730\\_0457](#) or later
- **JasperReports Server v9.0.0:** Apply HF9 - [hotfix\\_JRSP9.0.0\\_cumulative\\_20260730\\_0046](#) or later

Workarounds/ Mitigating Factors

None

What Cloud Software Group is Doing

Cloud Software Group is notifying customers and channel partners about this potential security issue through the publication of this security bulletin on the Jaspersoft Knowledge Center at <https://community.jaspersoft.com/advisories/>

Obtaining Support on This Issue

If you require technical assistance with this issue, please contact JasperSoft Technical Support. Contact details for JasperSoft Technical Support are available at <https://www.jaspersoft.com/contact-us>

Subscribe to Receive Alerts

Cloud Software Group strongly recommends that all customers subscribe to receive alerts when a Cloud Software Group security bulletin is created or modified at

<https://community.jaspersoft.com/advisories/>

## Reporting Security Vulnerabilities to Cloud Software Group

Jaspersoft welcomes input regarding the security of its products and considers any and all potential vulnerabilities seriously. For details on our vulnerability response process and guidance on how to report security-related issues to Jaspersoft, please see the following webpage:

<https://www.cloud.com/trust-center/support>

## Acknowledgement

Cloud Software Group Thanks Sonny of WatchTowr (<https://watchtowr.com/>) for working with us to protect Cloud Software Group customers

## Disclaimer

The information on this page is being provided to you on an "AS IS" and "AS-AVAILABLE" basis. The issues described on this page may or may not impact your system(s). Cloud Software Group, Inc. and its subsidiaries (collectively, "Cloud SG") make no representations, warranties, or guarantees as to the information contained herein. ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. BY ACCESSING THIS PAGE, YOU ACKNOWLEDGE THAT CLOUD SG SHALL IN NO EVENT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES THAT ARISE OUT OF YOUR USE OR FAILURE TO USE THE INFORMATION CONTAINED HEREIN. Cloud SG reserves the right to change or update the information on this page at any time. We accordingly recommend that you always view the latest version of this page. The information contained herein is being provided to you under the terms of your applicable customer agreement with Cloud SG, and may be used only for the purposes contemplated by such agreement. If you do not have such an agreement with Cloud SG, this information is provided under the [cloud.com](https://cloud.com/terms-of-use) Terms of Use, and may be used only for the purposes contemplated by such Terms of Use

## Change log

|            |                     |
|------------|---------------------|
| 2026-08-05 | Initial Publication |
|------------|---------------------|

 Share

 Followers

 Go to advisories



Contact Us

Cookies



© 2026 Actian, the data and AI division of  
HCLSoftware  
All rights reserved.

[Terms of Use](#)  
[Privacy Policy](#)  
[Cookie preferences](#)  
 [Your Privacy Choices](#) 

EXPLORE  
[Download Jaspersoft](#)

PRODUCTS

[Jaspersoft commercial edition](#)  
[Jaspersoft community edition](#)





Sign In



Join the Community



Search



Menu