



# CVE-2021-35495

Published on: 10/12/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

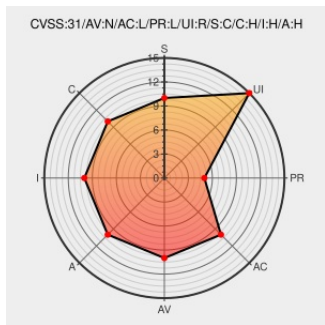
## CVE-2021-35495

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Jasperreports Server](#) from [Tibco](#) contain the following vulnerability:

The Scheduler Connection component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS

Marketplace, TIBCO JasperReports Server for ActiveMatrix BPM, and TIBCO JasperReports Server for Microsoft Azure contains an easily exploitable vulnerability that allows an authenticated attacker with network access to obtain FTP server passwords for other users of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 7.2.1 and below, TIBCO JasperReports Server: versions 7.5.0 and 7.5.1, TIBCO JasperReports Server: version 7.8.0, TIBCO JasperReports Server: version 7.9.0, TIBCO JasperReports Server - Community Edition: versions 7.8.0 and below, TIBCO JasperReports Server - Developer Edition: versions 7.9.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 7.9.0 and below, TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.9.0 and below, and TIBCO JasperReports Server for Microsoft Azure: version 7.8.0.

CVE-2021-35495 has been assigned by security@tibco.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **4 - MEDIUM**

Access Access Authentication

<b>Vector</b>	<b>Complexity</b>	
<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
<b>PARTIAL</b>	<b>NONE</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Advisory   TIBCO Software	<a href="https://web.archive.org">web.archive.org</a> <a href="#">text/html</a> Inactive Link Not Archived	 CONFIRM <a href="https://www.tibco.com/services/support/advisories">www.tibco.com/services/support/advisories</a>
TIBCO Security Advisory: October 12, 2021 - TIBCO JasperReports Server - 2021-35495   TIBCO Software	<a href="https://www.tibco.com">www.tibco.com</a> <a href="#">text/html</a>	 CONFIRM <a href="https://www.tibco.com/support/advisories/2021/10/tibco-security-advisory-october-12-2021-tibco-jasperreports-server-2021-35495">www.tibco.com/support/advisories/2021/10/tibco-security-advisory-october-12-2021-tibco-jasperreports-server-2021-35495</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Jasperreports Server	7.5.0	All	All	All
Application	Tibco	Jasperreports Server	7.5.1	All	All	All
Application	Tibco	Jasperreports Server	7.8.0	All	All	All
Application	Tibco	Jasperreports Server	7.9.0	All	All	All
Application	Tibco	Jasperreports Server	All	All	All	All
Application	Tibco	Jasperreports Server	All	All	All	All
Application	Tibco	Jasperreports Server	All	All	All	All
Application	Tibco	Jasperreports Server	All	All	All	All
Application	Tibco	Jasperreports Server	All	All	All	All
Application	Tibco	Jasperreports Server	All	All	All	All

- cpe:2.3:a:tibco:jasperreports\_server:7.5.0:\*:\*:\*:\*:\*:\*:
- cpe:2.3:a:tibco:jasperreports\_server:7.5.1:\*:\*:\*:\*:\*:\*:
- cpe:2.3:a:tibco:jasperreports\_server:7.8.0:\*:\*:\*:\*:\*:\*:
- cpe:2.3:a:tibco:jasperreports\_server:7.9.0:\*:\*:\*:\*:\*:\*:
- cpe:2.3:a:tibco:jasperreports\_server:\*:\*:\*:\*:\*:\*:

cpe:2.3:a:tibco:jasperreports\_server:\*:\*:\*:\*:microsoft\_azure:\*:\*:

cpe:2.3:a:tibco:jasperreports\_server:\*:\*:\*:\*:community:\*:\*:


cpe:2.3:a:tibco:jasperreports\_server:\*:\*:\*:\*:activematrix\_bpm:\*:\*:

cpe:2.3:a:tibco:jasperreports\_server:\*:\*:\*:\*:aws\_marketplace:\*:\*:

cpe:2.3:a:tibco:jasperreports\_server:\*:\*:\*:\*:developer:\*:\*:

No vendor comments have been submitted for this CVE

#### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-35495 : The Scheduler Connection component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO Jasp... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-10-12 17:41:07

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)