

CVE-2018-5430

TIBCO JasperReports Server Information Disclosure Vulnerability

CISA KEV since Dec 29, 2022

Actively exploited

The Spring web flows of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contain a vulnerability which may allow any authenticated user read-only access to the contents of the web application, including key configuration files.

EVRS 75/100 Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.481 98.9th percentile · FIRST	CISA DEADLINE Jan 19, 2023 KEV since 2022 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.481 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected releases include TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.2.4; 6.3.0; 6.3.2; 6.3.3; 6.4.0; 6.4.2, TIBCO JasperReports Server Community Edition: versions up to and including 6.4.2, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.2, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 6.4.2, TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 6.4.2.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jasperreports server	$\leq 6.2.4$ $\leq 6.4.2$ 6.3.0 6.3.2 6.3.3 6.4.0 6.4.2	after 6.2.4 · after 6.4.2	NVD
jaspersoft	$\leq 6.4.2$	after 6.4.2	NVD
jaspersoft reporting and analytics	$\leq 6.4.2$	after 6.4.2	NVD

Sources

Vendor guidance github.com/advisories/GHSA-782f-h7v4-m7wc

Additional guidance tibco.com/support/advisories/2018/04/tibco-security-advisory-april-17-2018-tibco-jasperreports-2018-5430

NVD nvd.nist.gov/vuln/detail/CVE-2018-5430

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-17200

Current data evulnable.com/vulnerability-management/cve/CVE-2018-5430

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.