



CVE-2015-5712

Published on: 10/28/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

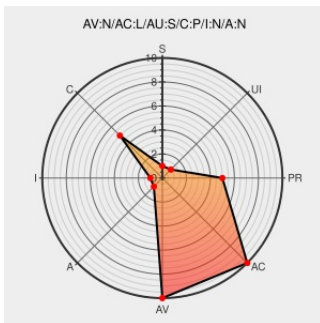
CVE-2015-5712

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Spotfire Analytics Platform For Aws](#) from [Tibco](#) contain the following vulnerability:

Spotfire Parsing Library and Spotfire Security Filter in TIBCO Spotfire Server 5.5.x before 5.5.4, 6.0.x before 6.0.5, 6.5.x before 6.5.4, and 7.0.x before 7.0.1 and Spotfire Analytics Platform before 7.0.2 for AWS Marketplace allow remote authenticated users to obtain sensitive system information by visiting an unspecified URL.

CVE-2015-5712 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

SINGLE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

TIBCO Spotfire Server Flaws Let Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker

www.securitytracker.com
[text/html](#)

[SECTrack 1034011](#)

Advisory | TIBCO Software

[Vendor Advisory](#)
www.tibco.com
[text/html](#)

[CONFIRM](#) www.tibco.com/mk/advisory.jsp

[Vendor Advisory](#)
www.tibco.com
[text/plain](#)

[CONFIRM](#) www.tibco.com/assets/blt3a3a55ab42f2f5cd/2015-004-advisory.txt

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,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Spotfire Analytics Platform For Aws	All	All	All	All
Application	Tibco	Spotfire Server	5.0.0	All	All	All
Application	Tibco	Spotfire Server	5.0.1	All	All	All
Application	Tibco	Spotfire Server	5.0.2	All	All	All
Application	Tibco	Spotfire Server	5.5.0	All	All	All
Application	Tibco	Spotfire Server	5.5.1	All	All	All
Application	Tibco	Spotfire Server	5.5.2	All	All	All
Application	Tibco	Spotfire Server	5.5.3	All	All	All
Application	Tibco	Spotfire Server	6.0.0	All	All	All
Application	Tibco	Spotfire Server	6.0.1	All	All	All
Application	Tibco	Spotfire Server	6.0.2	All	All	All
Application	Tibco	Spotfire Server	6.0.3	All	All	All
Application	Tibco	Spotfire Server	6.0.4	All	All	All
Application	Tibco	Spotfire Server	6.5.0	All	All	All
Application	Tibco	Spotfire Server	6.5.1	All	All	All
Application	Tibco	Spotfire Server	6.5.2	All	All	All
Application	Tibco	Spotfire Server	6.5.3	All	All	All
Application	Tibco	Spotfire Server	7.0.0	All	All	All
Application	Tibco	Spotfire Server	5.0.0	All	All	All
Application	Tibco	Spotfire Server	5.0.1	All	All	All
Application	Tibco	Spotfire Server	5.0.2	All	All	All
Application	Tibco	Spotfire Server	5.5.0	All	All	All
Application	Tibco	Spotfire Server	5.5.1	All	All	All
Application	Tibco	Spotfire Server	5.5.2	All	All	All
Application	Tibco	Spotfire Server	5.5.3	All	All	All
Application	Tibco	Spotfire Server	6.0.0	All	All	All
Application	Tibco	Spotfire Server	6.0.1	All	All	All
Application	Tibco	Spotfire Server	6.0.2	All	All	All
Application	Tibco	Spotfire Server	6.0.3	All	All	All
Application	Tibco	Spotfire Server	6.0.4	All	All	All

Application	Tibco	Spotfire Server	6.0.4	All	All	All
Application	Tibco	Spotfire Server	6.5.0	All	All	All
Application	Tibco	Spotfire Server	6.5.1	All	All	All
Application	Tibco	Spotfire Server	6.5.2	All	All	All
Application	Tibco	Spotfire Server	6.5.3	All	All	All
Application	Tibco	Spotfire Server	7.0.0	All	All	All
cpe:2.3:a:tibco:spotfire_analytics_platform_for_aws:*****:						
cpe:2.3:a:tibco:spotfire_server:5.0.0:*****:						
cpe:2.3:a:tibco:spotfire_server:5.0.1:*****:						
cpe:2.3:a:tibco:spotfire_server:5.0.2:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.0:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.1:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.2:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.3:*****:						
cpe:2.3:a:tibco:spotfire_server:6.0.0:*****:						
cpe:2.3:a:tibco:spotfire_server:6.0.1:*****:						
cpe:2.3:a:tibco:spotfire_server:6.0.2:*****:						
cpe:2.3:a:tibco:spotfire_server:6.0.3:*****:						
cpe:2.3:a:tibco:spotfire_server:6.0.4:*****:						
cpe:2.3:a:tibco:spotfire_server:6.5.0:*****:						
cpe:2.3:a:tibco:spotfire_server:6.5.1:*****:						
cpe:2.3:a:tibco:spotfire_server:6.5.2:*****:						
cpe:2.3:a:tibco:spotfire_server:6.5.3:*****:						
cpe:2.3:a:tibco:spotfire_server:7.0.0:*****:						
cpe:2.3:a:tibco:spotfire_server:5.0.0:*****:						
cpe:2.3:a:tibco:spotfire_server:5.0.1:*****:						
cpe:2.3:a:tibco:spotfire_server:5.0.2:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.0:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.1:*****:						
cpe:2.3:a:tibco:spotfire_server:5.5.2:*****:						

cpe:2.3:a:tibco:spotfire_server:5.5.3:*****:
cpe:2.3:a:tibco:spotfire_server:6.0.0:*****:
cpe:2.3:a:tibco:spotfire_server:6.0.1:*****:
cpe:2.3:a:tibco:spotfire_server:6.0.2:*****:
cpe:2.3:a:tibco:spotfire_server:6.0.3:*****:
cpe:2.3:a:tibco:spotfire_server:6.0.4:*****:
cpe:2.3:a:tibco:spotfire_server:6.5.0:*****:
cpe:2.3:a:tibco:spotfire_server:6.5.1:*****:
cpe:2.3:a:tibco:spotfire_server:6.5.2:*****:
cpe:2.3:a:tibco:spotfire_server:6.5.3:*****:
cpe:2.3:a:tibco:spotfire_server:7.0.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)