



CVE-2020-27146

Published on: 11/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:28 PM UTC

CVE-2020-27146

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L



Certain versions of [lprocess Workspace Browser](#) from [Tibco](#) contain the following vulnerability:

The Core component of TIBCO Software Inc.'s TIBCO iProcess Workspace (Browser) contains a vulnerability that theoretically allows an unauthenticated attacker with network access to execute a Cross Site Request Forgery (CSRF) attack on the affected system. A successful attack using this vulnerability requires human interaction from an authenticated user other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO iProcess Workspace (Browser): versions 11.6.0 and below.

CVE-2020-27146 has been assigned by [security@tibco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [TIBCO Software Inc.](#) - **TIBCO iProcess Workspace (Browser)** version <= 11.6.0

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link				
Advisory TIBCO Software	Vendor Advisory www.tibco.com text/html	 CONFIRM www.tibco.com/services/support/advisories				
TIBCO Security Advisory: November 10, 2020 - TIBCO iProcess Workspace Browser TIBCO Software	Vendor Advisory www.tibco.com text/html	 CONFIRM www.tibco.com/support/advisories/2020/11/tibco-security-advisory-november-10-2020-tibco-iprocess-workspace				
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.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Iprocess Workspace Browser	All	All	All	All
cpe:2.3:a:tibco:iprocess_workspace_browser:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID			Next ID →			