



# CVE-2016-10701

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2016-10701
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-11-28 01:29:00 UTC
<b>Updated</b>	2017-12-17 02:29:00 UTC
<b>Description</b>	In Hitachi Vantara Pentaho BA Platform through 8.0, a CSRF issue exists in the Business Analytics application.

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Hitachivantara</a>	<a href="#">Pentaho Business Analytics</a>	All	All	All	All

## References

Reference	Source	Link
[BISERVER-13207] CSRF Protection Built into Pentaho Application - Pentaho Platform Tracking	MISC	<a href="#">jira.pentaho.com</a>
[BISERVER-3562] As a system admin, I want the pentaho server to run with Tomcat 7. - Pentaho Platform Tracking	MISC	<a href="#">jira.pentaho.com</a>
[BISERVER-6599] Upgrade to Tomcat 7, and incorporate the CSRF prevention filter - Pentaho Platform Tracking	MISC	<a href="#">jira.pentaho.com</a>
Hitachi Vantara Pentaho BA Platform CVE-2016-10701 Cross Site Request Forgery Vulnerability	BID	<a href="#">www.securityfocus.com/bid/78441</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org/CVE/2016/10701</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov/vuln/detail/CVE-2016-10701</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)