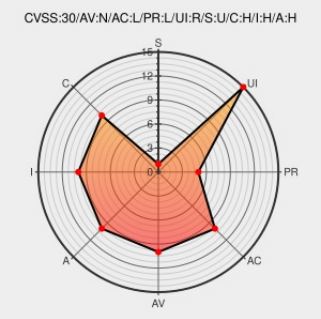
CVE-2018-7216

Published on: 02/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7216

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bravo Solution from Tejari contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in esop/toolkit/profile/regData.do in Bravo Tejari Procurement Portal allows remote authenticated users to hijack the authentication of application users for requests that modify their personal data by leveraging lack of anti-CSRF tokens.

CVE-2018-7216 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com	MISC www.securityfocus.com/archive/1/541782/30/0/threaded

	text/html	
Tejari Cross Site Request Forgery ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/146409/Tejari-Cross-Site-Request-Forgery.html
Full Disclosure: : Vulnerability Disclosure (Web Apps)-Bravo Tejari Web Portal-CSRF	Exploit Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2018/Feb/44
Bravo Tejari Web Portal - Cross-Site Request Forgery - Multiple webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 44256

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	Tejari	Bravo Solution	-	All	All	All
Application	Tejari	Bravo Solution	-	All	All	All

cpe:2.3:a:tejari:bravo_solution:-:*:*:*:*:*:*:*:

cpe:2.3:a:tejari:bravo_solution:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→