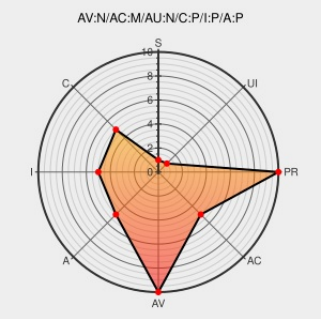
CVE-2012-5950

Published on: 04/23/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:21 PM UTC

CVE-2012-5950

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



Certain versions of Tririga Application Platform from Ibm contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in IBM TRIRIGA Application Platform 2.x and 3.x before 3.3, and 8, allow remote attackers to hijack the authentication of arbitrary users for requests that modify data records via vectors involving (1) the html/en/default/ directory or (2) sqa/html/en/default/process/comm/saveProps.jsp.

CVE-2012-5950 has been assigned by psirt@us.ibm.com to track the vulnerability

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
IBM TRIRIGA Application Platform Cross Site Request Forgery vulnerabilities. - United States	Vendor Advisory www-01.ibm.com text/html	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21628849
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tririga-csrf(80630)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tririga Application Platform	2.1	All	All	All
Application	Ibm	Tririga Application Platform	2.5	All	All	All
Application	Ibm	Tririga Application Platform	2.6	All	All	All
Application	Ibm	Tririga Application Platform	2.7	All	All	All
Application	Ibm	Tririga Application Platform	3.0	All	All	All
Application	Ibm	Tririga Application Platform	3.1	All	All	All
Application	Ibm	Tririga Application Platform	3.2	All	All	All
Application	Ibm	Tririga Application Platform	3.2.1	All	All	All
Application	Ibm	Tririga Application Platform	8.0	All	All	All
Application	Ibm	Tririga Application Platform	2.1	All	All	All
Application	Ibm	Tririga Application Platform	2.5	All	All	All
Application	Ibm	Tririga Application Platform	2.6	All	All	All
Application	Ibm	Tririga Application Platform	2.7	All	All	All
Application	Ibm	Tririga Application Platform	3.0	All	All	All
Application	Ibm	Tririga Application Platform	3.1	All	All	All
Application	Ibm	Tririga Application Platform	3.2	All	All	All
Application	Ibm	Tririga Application Platform	3.2.1	All	All	All
Application	Ibm	Tririga Application Platform	8.0	All	All	All

cpe:2.3:a:ibm:tririga_application_platform:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:2.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:2.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:3.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tririga_application_platform:2.6:*:*:*:*:*:*:*

cpe:2.3:a:ibm:tririga_application_platform:2.7:*:*:*:*:*:*:*

cpe:2.3:a:ibm:tririga_application_platform:3.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:tririga_application_platform:3.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:tririga_application_platform:3.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:tririga_application_platform:3.2.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:tririga_application_platform:8.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→