



CVE-2014-4838

Published on: 10/18/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-4838

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

Certain versions of [Tririga Application Platform](#) from [Ibm](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in GanttProjectSchedulerPopup.jsp in IBM TRIRIGA Application Platform 3.2 and 3.3 before 3.3.0.2, 3.3.1 before 3.3.1.3, 3.3.2 before 3.3.2.2, and 3.4 before 3.4.0.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.

CVE-2014-4838 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

SINGLE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

Security Advisory SA61056 - IBM TRIRIGA Application Platform Multiple Vulnerabilities - Secunia

[web.archive.org](#)
[text/html](#)

[SECUNIA 61056](#)

IBM notice: The page you requested cannot be displayed

[Vendor Advisory](#)
[www-01.ibm.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21686233](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF ibm-tririga-cve20144838-xss\(95634\)](#)

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

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	3.2	All	All	All
Application	ibm	Tririga Application Platform	3.2.1	All	All	All
Application	ibm	Tririga Application Platform	3.3.0.0	All	All	All
Application	ibm	Tririga Application Platform	3.3.0.1	All	All	All
Application	ibm	Tririga Application Platform	3.3.1.0	All	All	All
Application	ibm	Tririga Application Platform	3.3.1.1	All	All	All
Application	ibm	Tririga Application Platform	3.3.1.2	All	All	All
Application	ibm	Tririga Application Platform	3.3.2.0	All	All	All
Application	ibm	Tririga Application Platform	3.3.2.1	All	All	All
Application	ibm	Tririga Application Platform	3.4.0.0	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	3.3.0.0	All	All	All
Application	ibm	Tririga Application Platform	3.3.0.1	All	All	All
Application	ibm	Tririga Application Platform	3.3.1.0	All	All	All
Application	ibm	Tririga Application Platform	3.3.1.1	All	All	All
Application	ibm	Tririga Application Platform	3.3.1.2	All	All	All
Application	ibm	Tririga Application Platform	3.3.2.0	All	All	All
Application	ibm	Tririga Application Platform	3.3.2.1	All	All	All
Application	ibm	Tririga Application Platform	3.4.0.0	All	All	All
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:3.3.0.0:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.3.0.1:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.3.1.0:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.3.1.1:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.3.1.2:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.3.2.0:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.3.2.1:*:*:*:*:*:						
cpe:2.3:a:ibm:tririga_application_platform:3.4.0.0:*:*:*:*:*:						

cpe:2.3:a:ibm:tririga_application_platform:3.3.2.1:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.4.0.0:*****:
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:3.3.0.0:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.3.0.1:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.3.1.0:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.3.1.1:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.3.1.2:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.3.2.0:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.3.2.1:*****:
cpe:2.3:a:ibm:tririga_application_platform:3.4.0.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)