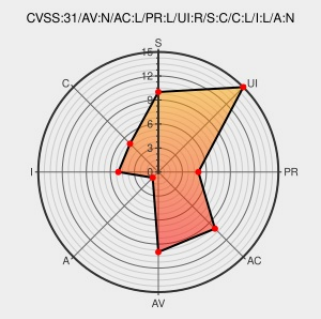
CVE-2021-29814

Published on: 09/23/2021 12:00:00 AM UTC

Last Modified on: 09/27/2021 08:57:00 PM UTC

CVE-2021-29814

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



Certain versions of Aix from Ibm contain the following vulnerability:

IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204334.

CVE-2021-29814 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **IBM** - **Jazz for Service Management** version **1.1.3.10**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Security Bulletin: IBM Jazz for Service Management is	www.ibm.com	CONFIRM

vulnerable to stored cross-site scripting (CVE-2021-29814)	text/html	www.ibm.com/support/pages/node/6491539
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-tivoli-cve202129814-xss (204334)

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
Operating System	Ibm	Aix	-	All	All	All
Application	Ibm	Jazz For Service Management	1.1.3.10	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:o:ibm:aix:-:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:jazz_for_service_management:1.1.3.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-29814 : #IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stor… twitter.com/i/web/status/1…	2021-09-23 18:09:47
@0_exploit	CVE-2021-29814 dlvr.it/S89Kly	2021-09-23 23:01:09
@SecRiskRptSME	RT: CVE-2021-29814 IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to st… twitter.com/i/web/status/1…	2021-09-24 07:33:50

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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 registred 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.

CVE.report and Source URL Uptime Status status.cve.report