

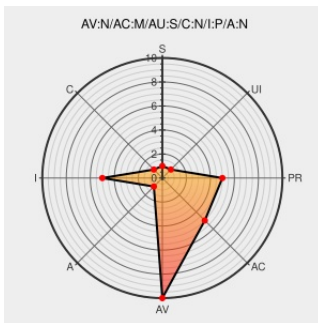


CVE-2014-6215

Published on: 12/11/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:55 PM UTC

CVE-2014-6215

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

Certain versions of [Websphere Portal](#) from [ibm](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0.0 before 7.0.0.2 CF29, 8.0.0 through 8.0.0.1 CF14, and 8.5.0 before CF03 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.

CVE-2014-6215 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

IBM X-Force Exchange

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

[XF ibm-wsportal-cve20146215-xss\(98802\)](#)

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=swg21691458](#)

IBM notice: The page you requested cannot be displayed

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

[AIXAPAR PI24434](#)

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,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Portal	6.1.0	All	All	All
Application	Ibm	Websphere Portal	6.1.0.1	All	All	All
Application	Ibm	Websphere Portal	6.1.0.2	All	All	All
Application	Ibm	Websphere Portal	6.1.0.3	All	All	All
Application	Ibm	Websphere Portal	6.1.0.4	All	All	All
Application	Ibm	Websphere Portal	6.1.0.5	All	All	All
Application	Ibm	Websphere Portal	6.1.0.6	All	All	All
Application	Ibm	Websphere Portal	6.1.0.6	cf27	All	All
Application	Ibm	Websphere Portal	7.0.0	All	All	All
Application	Ibm	Websphere Portal	7.0.0.1	All	All	All
Application	Ibm	Websphere Portal	7.0.0.2	All	All	All
Application	Ibm	Websphere Portal	8.0.0	All	All	All
Application	Ibm	Websphere Portal	8.0.0.1	All	All	All
Application	Ibm	Websphere Portal	8.0.0.1	14	All	All
Application	Ibm	Websphere Portal	8.5.0	All	All	All
Application	Ibm	Websphere Portal	6.1.0	All	All	All
Application	Ibm	Websphere Portal	6.1.0.1	All	All	All
Application	Ibm	Websphere Portal	6.1.0.2	All	All	All
Application	Ibm	Websphere Portal	6.1.0.3	All	All	All
Application	Ibm	Websphere Portal	6.1.0.4	All	All	All
Application	Ibm	Websphere Portal	6.1.0.5	All	All	All
Application	Ibm	Websphere Portal	6.1.0.6	All	All	All
Application	Ibm	Websphere Portal	6.1.0.6	cf27	All	All
Application	Ibm	Websphere Portal	7.0.0	All	All	All
Application	Ibm	Websphere Portal	7.0.0.1	All	All	All
Application	Ibm	Websphere Portal	7.0.0.2	All	All	All
Application	Ibm	Websphere Portal	8.0.0	All	All	All
Application	Ibm	Websphere Portal	8.0.0.1	All	All	All
Application	Ibm	Websphere Portal	8.0.0.1	14	All	All
Application	Ibm	Websphere Portal	8.5.0	All	All	All

Application	IBM	websphere Portal	6.5.0	All	All	All
		cpe:2.3:a:ibm:websphere_portal:6.1.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.1:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.2:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.3:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.4:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.5:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.6:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.6:cf27:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:7.0.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:7.0.0.1:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:7.0.0.2:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:8.0.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:8.0.0.1:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:8.0.0.1:14:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:8.5.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.1:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.2:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.3:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.4:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.5:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.6:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:6.1.0.6:cf27:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:7.0.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:7.0.0.1:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:7.0.0.2:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:8.0.0:*:*:*:*:*:				
		cpe:2.3:a:ibm:websphere_portal:8.0.0.1:*:*:*:*:*:				

cpe:2.3:a:ibm:websphere_portal:8.0.0.1:14:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_portal:8.5.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)