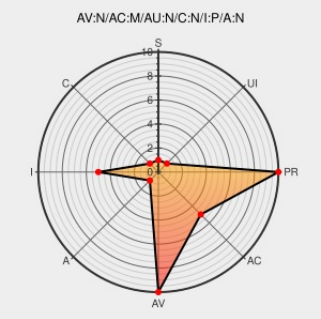
CVE-2014-6171

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

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

CVE-2014-6171

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 through 7.0.0.2 CF29, 8.0.0 through 8.0.0.1 CF14, and 8.5.0 before CF04 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

CVE-2014-6171 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-wsportal-cve20146171-xss(98383)
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=swg21692107
IBM notice: The page you requested cannot be displayed	Vendor Advisory www-01.ibm.com text/html Inactive Link Not Archived	AIXAPAR PI29134

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	Ibm	Websphere Portal	6.1.0.0	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	6.1.5.0	All	All	All
Application	Ibm	Websphere Portal	6.1.5.1	All	All	All
Application	Ibm	Websphere Portal	6.1.5.2	All	All	All
Application	Ibm	Websphere Portal	6.1.5.3	All	All	All
Application	Ibm	Websphere Portal	7.0.0.0	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	8.0.0.0	All	All	All
Application	Ibm	Websphere Portal	8.0.0.1	All	All	All
Application	Ibm	Websphere Portal	8.5.0.0	All	All	All
Application	Ibm	Websphere Portal	6.1.0.0	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	6.1.5.0	All	All	All
Application	Ibm	Websphere Portal	6.1.5.1	All	All	All
Application	Ibm	Websphere Portal	6.1.5.2	All	All	All
Application	Ibm	Websphere Portal	6.1.5.3	All	All	All
Application	Ibm	Websphere Portal	7.0.0.0	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	8.0.0.0	All	All	All
Application	Ibm	Websphere Portal	8.0.0.1	All	All	All
Application	Ibm	Websphere Portal	8.5.0.0	All	All	All

cpe:2.3:a:ibm:websphere_portal:6.1.0.0:*:*:*:*:*:*:*

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:6.1.5.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.5.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.5.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.5.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:7.0.0.0:*:*:*:*:*:*:*

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:8.0.0.0:*:*:*:*:*:*:*

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

cpe:2.3:a:ibm:websphere_portal:8.5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.0.0:*:*:*:*:*:*:*

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:6.1.5.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.5.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.5.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:6.1.5.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:websphere_portal:7.0.0.0:*:*:*:*:*:*:*

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:8.0.0.0:*:*:*:*:*:*:*

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

cpe:2.3:a:ibm:websphere_portal:8.5.0.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→