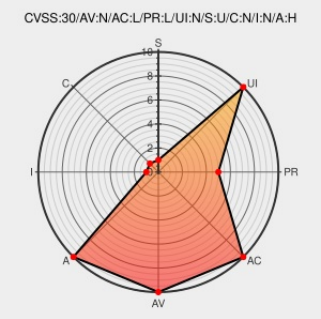
CVE-2016-5954

Published on: 09/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5954

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



Certain versions of Websphere Portal from Ibm contain the following vulnerability:

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 CF30, 8.0.0 through 8.0.0.1 CF21, and 8.5.0 before CF12 allows remote authenticated users to cause a denial of service by uploading temporary files.

CVE-2016-5954 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
IBM Security Bulletin: Security vulnerability has been identified in IBM WebSphere Portal (CVE-2016-5954) - United States	Patch, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21989993

IBM WebSphere Portal Temporary File Uploading Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036762
IBM notice: The page you requested cannot be displayed	Not Applicable www-01.ibm.com text/html Inactive Link Not Archived	AIXAPAR PI67037
IBM WebSphere Portal CVE-2016-5954 Denial of Service Vulnerability	cve.report (archive) text/html	BID 93017

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→