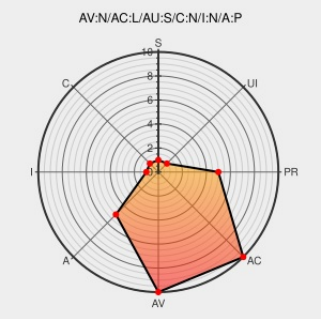
CVE-2012-0712

Published on: 03/20/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:24 PM UTC

CVE-2012-0712

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



Certain versions of Db2 from Ibm contain the following vulnerability:

The XML feature in IBM DB2 9.5 before FP9, 9.7 through FP5, and 9.8 through FP4 allows remote authenticated users to cause a denial of service (infinite loop) by calling the XMLPARSE function with a crafted string expression.

CVE-2012-0712 has been assigned by psirt@us.ibm.com to track the vulnerability

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 X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF db2-xmlfeature-dos(73496)
IBM IC81379: SECURITY: DENIAL OF SERVICE SECURITY VULNERABILITY IN DB2'S XML FEATURE (CVE-2012-0712).	www-01.ibm.com text/html	AIXAPAR IC81379
IBM IC81380: SECURITY: DENIAL OF SERVICE SECURITY VULNERABILITY IN DB2'S XML FEATURE (CVE-2012-0712).	www-01.ibm.com text/html	AIXAPAR IC81380
IBM IC81837: SECURITY: DENIAL OF SERVICE SECURITY VULNERABILITY IN DB2'S XML FEATURE (CVE-2012-0712).	www-01.ibm.com text/html	AIXAPAR IC81837
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:14450
IBM Security Bulletin: Denial of Service Security Vulnerability in DB2's XML Feature. (CVE-2012-0712) - United States	Vendor Advisory www-01.ibm.com	CONFIRM www-01.ibm.com/support/docview.wss?

text/html uid=swg21588098

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	Db2	9.5	All	All	All
Application	Ibm	Db2	9.5	fp1	All	All
Application	Ibm	Db2	9.5	fp2	All	All
Application	Ibm	Db2	9.5	fp2a	All	All
Application	Ibm	Db2	9.5	fp3	All	All
Application	Ibm	Db2	9.5	fp3a	All	All
Application	Ibm	Db2	9.5	fp3b	All	All
Application	Ibm	Db2	9.5	fp4	All	All
Application	Ibm	Db2	9.5	fp4a	All	All
Application	Ibm	Db2	9.5	fp5	All	All
Application	Ibm	Db2	9.5	fp6	All	All
Application	Ibm	Db2	9.5	fp6a	All	All
Application	Ibm	Db2	9.5	fp7	All	All
Application	Ibm	Db2	9.5	fp8	All	All
Application	Ibm	Db2	9.7	All	All	All
Application	Ibm	Db2	9.7	fp1	All	All
Application	Ibm	Db2	9.7	fp2	All	All
Application	Ibm	Db2	9.7	fp3	All	All
Application	Ibm	Db2	9.7	fp3a	All	All
Application	Ibm	Db2	9.7	fp4	All	All
Application	Ibm	Db2	9.7	fp5	All	All
Application	Ibm	Db2	9.8	All	All	All
Application	Ibm	Db2	9.8	fp3	All	All
Application	Ibm	Db2	9.8	fp4	All	All
Application	Ibm	Db2	9.5	All	All	All
Application	Ibm	Db2	9.5	fp1	All	All
Application	Ibm	Db2	9.5	fp2	All	All

Application	Ibm	Db2	9.5	fp2a	All	All
Application	Ibm	Db2	9.5	fp3	All	All
Application	Ibm	Db2	9.5	fp3a	All	All
Application	Ibm	Db2	9.5	fp3b	All	All
Application	Ibm	Db2	9.5	fp4	All	All
Application	Ibm	Db2	9.5	fp4a	All	All
Application	Ibm	Db2	9.5	fp5	All	All
Application	Ibm	Db2	9.5	fp6	All	All
Application	Ibm	Db2	9.5	fp6a	All	All
Application	Ibm	Db2	9.5	fp7	All	All
Application	Ibm	Db2	9.5	fp8	All	All
Application	Ibm	Db2	9.7	All	All	All
Application	Ibm	Db2	9.7	fp1	All	All
Application	Ibm	Db2	9.7	fp2	All	All
Application	Ibm	Db2	9.7	fp3	All	All
Application	Ibm	Db2	9.7	fp3a	All	All
Application	Ibm	Db2	9.7	fp4	All	All
Application	Ibm	Db2	9.7	fp5	All	All
Application	Ibm	Db2	9.8	All	All	All
Application	Ibm	Db2	9.8	fp3	All	All
Application	Ibm	Db2	9.8	fp4	All	All

cpe:2.3:a:ibm:db2:9.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp2a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp3b:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp4a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp6:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp6a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp7:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp8:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.8:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.8:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp2a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp3b:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp4a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp6:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp6a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp7:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.5:fp8:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.8:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.8:fp4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→