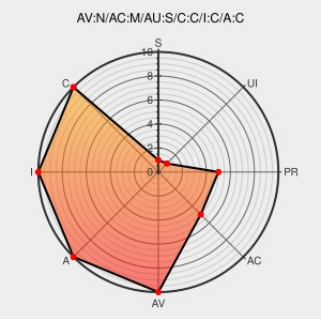
CVE-2013-6744

Published on: 05/30/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

CVE-2013-6744

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



Certain versions of Db2 from Ibm contain the following vulnerability:

The Stored Procedure infrastructure in IBM DB2 9.5, 9.7 before FP9a, 10.1 before FP3a, and 10.5 before FP3a on Windows allows remote authenticated users to gain privileges by leveraging the CONNECT privilege and the CREATE_EXTERNAL_ROUTINE authority.

CVE-2013-6744 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
IC99481: SECURITY: VULNERABILITY IN STORED PROCEDURE INFRASTRUCTURE CAN ALLOW ESCALATION OF PRIVILEGE TO ADMINISTRATOR (CVE-2013-6744).	www-01.ibm.com text/html	AIXAPAR IC99481
IC99478: SECURITY: VULNERABILITY IN STORED PROCEDURE INFRASTRUCTURE CAN ALLOW ESCALATION OF PRIVILEGE TO ADMINISTRATOR (CVE-2013-6744).	www-01.ibm.com text/html	AIXAPAR IC99478
Security Vulnerabilities, HIPER and Special Attention APARs fixed in DB2 for Linux, UNIX, and Windows Version 10.1	www.ibm.com text/html	CONFIRM www.ibm.com/support/docview.wss?uid=swg21610582#4
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-db2-cve20136744-priv-escalation(89860)
IC99480: SECURITY: VULNERABILITY IN STORED PROCEDURE INFRASTRUCTURE CAN ALLOW ESCALATION OF PRIVILEGE TO	Vendor Advisory www.ibm.com	CONFIRM www.ibm.com/support/docview.wss?

ADMINISTRATOR (CVE-2013-6744).	text/html	uid=swg1IC99480
IC99480: SECURITY: VULNERABILITY IN STORED PROCEDURE INFRASTRUCTURE CAN ALLOW ESCALATION OF PRIVILEGE TO ADMINISTRATOR (CVE-2013-6744).	www-01.ibm.com text/html	AIXAPAR IC99480
Security Bulletin: Escalation of Privilege Vulnerability in IBM® DB2® Stored Procedure Infrastructure on Windows (CVE-2013-6744)	www.ibm.com text/html	CONFIRM www.ibm.com/support/docview.wss?uid=swg21673947
No Description Provided	www-01.ibm.com text/html	AIXAPAR IC98849

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	10.1	All	All	All
Application	Ibm	Db2	10.1.0.1	All	All	All
Application	Ibm	Db2	10.1.0.2	All	All	All
Application	Ibm	Db2	10.1.0.3	All	All	All
Application	Ibm	Db2	10.5	All	All	All
Application	Ibm	Db2	10.5.0.1	All	All	All
Application	Ibm	Db2	10.5.0.2	All	All	All
Application	Ibm	Db2	9.5	All	All	All
Application	Ibm	Db2	9.7	All	All	All
Application	Ibm	Db2	9.7.0.1	All	All	All
Application	Ibm	Db2	9.7.0.2	All	All	All
Application	Ibm	Db2	9.7.0.3	All	All	All
Application	Ibm	Db2	9.7.0.4	All	All	All
Application	Ibm	Db2	9.7.0.5	All	All	All
Application	Ibm	Db2	9.7.0.6	All	All	All
Application	Ibm	Db2	9.7.0.7	All	All	All
Application	Ibm	Db2	9.7.0.8	All	All	All
Application	Ibm	Db2	9.7.0.9	All	All	All
Application	Ibm	Db2	10.1	All	All	All
Application	Ibm	Db2	10.1.0.1	All	All	All
Application	Ibm	Db2	10.1.0.2	All	All	All

Application	Ibm	Db2	10.1.0.3	All	All	All
Application	Ibm	Db2	10.5	All	All	All
Application	Ibm	Db2	10.5.0.1	All	All	All
Application	Ibm	Db2	10.5.0.2	All	All	All
Application	Ibm	Db2	9.5	All	All	All
Application	Ibm	Db2	9.7	All	All	All
Application	Ibm	Db2	9.7.0.1	All	All	All
Application	Ibm	Db2	9.7.0.2	All	All	All
Application	Ibm	Db2	9.7.0.3	All	All	All
Application	Ibm	Db2	9.7.0.4	All	All	All
Application	Ibm	Db2	9.7.0.5	All	All	All
Application	Ibm	Db2	9.7.0.6	All	All	All
Application	Ibm	Db2	9.7.0.7	All	All	All
Application	Ibm	Db2	9.7.0.8	All	All	All
Application	Ibm	Db2	9.7.0.9	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All

cpe:2.3:a:ibm:db2:10.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.2:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:ibm:db2:9.7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.2:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:ibm:db2:9.7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.9:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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