



CVE-2010-3194

Published on: 08/31/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:02 PM UTC

CVE-2010-3194

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

Certain versions of [Db2](#) from [ibm](#) contain the following vulnerability:

The DB2DART program in IBM DB2 9.1 before FP9, 9.5 before FP6, and 9.7 before FP2 allows attackers to bypass intended file access restrictions via unspecified vectors related to overwriting files owned by an instance owner.

CVE-2010-3194 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
www.vupen.com
[text/html](#)

[VUPEN ADV-2010-2225](#)

IBM IC65756: Security: DB2DART PROGRAM COULD OVERWRITE FILES OWNED BY THE INSTANCE OWNER. - United States

[Vendor Advisory](#)
www-01.ibm.com
[text/html](#)

[AIXAPAR IC65756](#)

IBM IC65762: Security: DB2DART PROGRAM COULD OVERWRITE FILES OWNED BY THE INSTANCE OWNER. - United States

[Vendor Advisory](#)
www-01.ibm.com
[text/html](#)

[AIXAPAR IC65762](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval:org.mitre.oval:def:13841](#)

public.dhe.ibm.com
[text/plain](#)

[CONFIRM](#)
public.dhe.ibm.com/ps/products/db2/fixes/english-

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
[text/html](#)
 XF db2-db2dart-priv-escalation(61445)

IBM - Security Vulnerabilities and HIPER APARs fixed in DB2 for Linux, UNIX, and Windows Version 9.7 Fix Pack 2

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)
 CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21432298

IBM - Security Vulnerabilities and HIPER APARs fixed in DB2 for Linux, UNIX, and Windows Version 9.1 Fix Pack 9

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)
 CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21426108

IBM DB2 Multiple Vulnerabilities - Advisories - Community

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
 SECUNIA 41218

IBM IC65749: Security: DB2DART PROGRAM COULD OVERWRITE FILES OWNED BY THE INSTANCE OWNER. - United States

[www-01.ibm.com](#)
[text/html](#)
 AIXAPAR IC65749

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	9.1	All	All	All
Application	Ibm	Db2	9.1	fp1	All	All
Application	Ibm	Db2	9.1	fp2	All	All
Application	Ibm	Db2	9.1	fp2a	All	All
Application	Ibm	Db2	9.1	fp3	All	All
Application	Ibm	Db2	9.1	fp3a	All	All
Application	Ibm	Db2	9.1	fp4	All	All
Application	Ibm	Db2	9.1	fp4a	All	All
Application	Ibm	Db2	9.1	fp5	All	All
Application	Ibm	Db2	9.1	fp6	All	All
Application	Ibm	Db2	9.1	fp6a	All	All
Application	Ibm	Db2	9.1	fp7	All	All
Application	Ibm	Db2	9.1	fp7a	All	All
Application	Ibm	Db2	9.1	fp8	All	All
Application	Ibm	Db2	9.5	All	All	All
Application	Ibm	Db2	9.5	fp1	All	All

Application	lbm	Db2	9.5	fp2	All	All
Application	lbm	Db2	9.5	fp2a	All	All
Application	lbm	Db2	9.5	fp3	All	All
Application	lbm	Db2	9.5	fp3a	All	All
Application	lbm	Db2	9.5	fp3b	All	All
Application	lbm	Db2	9.5	fp4	All	All
Application	lbm	Db2	9.5	fp4a	All	All
Application	lbm	Db2	9.5	fp5	All	All
Application	lbm	Db2	9.7	All	All	All
Application	lbm	Db2	9.7	fp1	All	All
Application	lbm	Db2	9.1	All	All	All
Application	lbm	Db2	9.1	fp1	All	All
Application	lbm	Db2	9.1	fp2	All	All
Application	lbm	Db2	9.1	fp2a	All	All
Application	lbm	Db2	9.1	fp3	All	All
Application	lbm	Db2	9.1	fp3a	All	All
Application	lbm	Db2	9.1	fp4	All	All
Application	lbm	Db2	9.1	fp4a	All	All
Application	lbm	Db2	9.1	fp5	All	All
Application	lbm	Db2	9.1	fp6	All	All
Application	lbm	Db2	9.1	fp6a	All	All
Application	lbm	Db2	9.1	fp7	All	All
Application	lbm	Db2	9.1	fp7a	All	All
Application	lbm	Db2	9.1	fp8	All	All
Application	lbm	Db2	9.5	All	All	All
Application	lbm	Db2	9.5	fp1	All	All
Application	lbm	Db2	9.5	fp2	All	All
Application	lbm	Db2	9.5	fp2a	All	All
Application	lbm	Db2	9.5	fp3	All	All
Application	lbm	Db2	9.5	fp3a	All	All
Application	lbm	Db2	9.5	fp3b	All	All
Application	lbm	Db2	9.5	fp4	All	All
Application	lbm	Db2	9.5	fp4a	All	All
Application	lbm	Db2	9.5	fp5	All	All
Application	lbm	Db2	9.7	All	All	All

Application	lbm	Db2	9.7	fp1	All	All
						cpe:2.3:a:ibm:db2:9.1:*****:
						cpe:2.3:a:ibm:db2:9.1:fp1:*****:
						cpe:2.3:a:ibm:db2:9.1:fp2:*****:
						cpe:2.3:a:ibm:db2:9.1:fp2a:*****:
						cpe:2.3:a:ibm:db2:9.1:fp3:*****:
						cpe:2.3:a:ibm:db2:9.1:fp3a:*****:
						cpe:2.3:a:ibm:db2:9.1:fp4:*****:
						cpe:2.3:a:ibm:db2:9.1:fp4a:*****:
						cpe:2.3:a:ibm:db2:9.1:fp5:*****:
						cpe:2.3:a:ibm:db2:9.1:fp6:*****:
						cpe:2.3:a:ibm:db2:9.1:fp6a:*****:
						cpe:2.3:a:ibm:db2:9.1:fp7:*****:
						cpe:2.3:a:ibm:db2:9.1:fp7a:*****:
						cpe:2.3:a:ibm:db2:9.1:fp8:*****:
						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:db2:9.7:*****:
						cpe:2.3:a:ibm:db2:9.7:fp1:*****:
						cpe:2.3:a:ibm:db2:9.1:*****:
						cpe:2.3:a:ibm:db2:9.1:fp1:*****:

cpe:2.3:a:ibm:db2:9.1:fp2:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp2a:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp3:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp3a:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp4:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp4a:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp5:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp6:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp6a:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp7:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp7a:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.1:fp8:~::~~::~~::~~::
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:db2:9.7:~::~~::~~::~~::
cpe:2.3:a:ibm:db2:9.7:fp1:~::~~::~~::~~::

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](#)