



CVE-2004-1372

Published on: 09/01/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

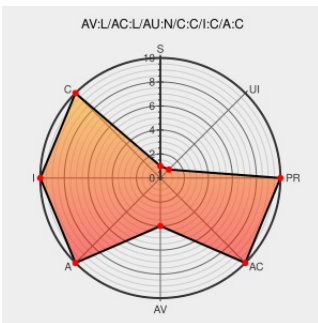
CVE-2004-1372

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Db2 Universal Database](#) from [Ibm](#) contain the following vulnerability:

Multiple stack-based buffer overflows in IBM DB2 7.x and 8.1 allow local users to execute arbitrary code via (1) a long third argument to the rec2xml function or (2) a long filename argument to the generate_distfile procedure.

CVE-2004-1372 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access Vector

Access Complexity

Authentication

LOCAL

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Patch
Vendor Advisory
[www.ngssoftware.com](#)
text/plain
Inactive Link Not Archived

MISC
[www.ngssoftware.com/advisories/db223122004L.txt](#)

Patch
Vendor Advisory
[www.ngssoftware.com](#)
text/plain
Inactive Link Not Archived

MISC
[www.ngssoftware.com/advisories/db223122004K.txt](#)

IBM DB2 Universal Database REC2XML and GENERATE_DISTFILE Buffer Overflow Vulnerabilities

Patch
cve.report (archive)
text/html

BID 11089

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#) XF db2-generatedistfile-bo(18663)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

'IBM DB2 rec2xml buffer overflow vulnerability (#NISR2122004J)' - MARC

marc.info

text/html

BUGTRAQ 20041223 IBM DB2 rec2xml buffer overflow vulnerability (#NISR2122004J)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

XF db2-rec2xml-bo(18682)

'IBM DB2 generate_distfile buffer overflow vulnerability (#NISR2122004L)' - MARC

marc.info

text/html

BUGTRAQ 20041223 IBM DB2 generate_distfile buffer overflow vulnerability (#NISR2122004L)

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 Universal Database	7.0	All	linux	All
Application	ibm	Db2 Universal Database	7.1	All	linux	All
Application	ibm	Db2 Universal Database	7.2	All	linux	All
Application	ibm	Db2 Universal Database	8.1	All	aix	All
Application	ibm	Db2 Universal Database	7.0	All	linux	All
Application	ibm	Db2 Universal Database	7.1	All	linux	All
Application	ibm	Db2 Universal Database	7.2	All	linux	All
Application	ibm	Db2 Universal Database	8.1	All	aix	All
cpe:2.3:a:ibm:db2_universal_database:7.0:*:linux:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:7.1:*:linux:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:7.2:*:linux:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:8.1:*:aix:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:7.0:*:linux:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:7.1:*:linux:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:7.2:*:linux:*:*:*:*:						
cpe:2.3:a:ibm:db2_universal_database:8.1:*:aix:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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](#)