



CVE-2010-0472

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-0472
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-02-02 18:30:00 UTC
Updated	2017-09-19 01:30:00 UTC
Description	kuddb2 in Tivoli Monitoring for DB2, as distributed in IBM DB2 9.7 FP1 on Linux, allows remote attackers to cause a denial

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Db2	9.7.0.1	All	linux	All
Application	ibm	Db2	9.7.0.1	All	linux	All

References

Reference	Source
Repository / Oval Repository	OVAL
IBM DB2 'kuddb2' Remote Denial of Service Vulnerability	BID
IC68762: SECURITY: THE TIVOLI MONITORING AGENT (KUDDDB2) FOR DB2 HAS DOS VULNERABILITY. (CVE-2010-0472)	AIXAPAR
IBM - Security Vulnerabilities and HIPER APARs fixed in DB2 for Linux, UNIX, and Windows Version 9.7 Fix Pack 2	CONFIRM
Intevydis blog: IBM DB2 9.7 kuddb2 DoS	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)