



CVE-2007-1228

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

Summary

CVE	CVE-2007-1228
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-02 22:19:00 UTC
Updated	2009-02-11 05:00:00 UTC
Description	IBM DB2 UDB 8.2 before Fixpak 7 (aka fixpack 14), and DB2 9 before Fix Pack 2, on UNIX allows the "fenced" user to acc

Risk And Classification

Problem Types: CWE-287

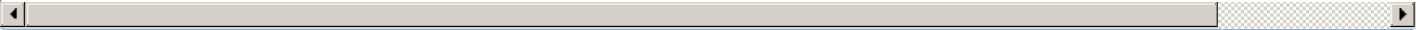
NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Db2	8.2	All	All	All
Application	ibm	Db2	8.2	fp1	All	All
Application	ibm	Db2	8.2	fp2	All	All
Application	ibm	Db2	8.2	fp3	All	All
Application	ibm	Db2	8.2	fp4	All	All
Application	ibm	Db2	8.2	fp5	All	All
Application	ibm	Db2	8.2	fp6	All	All
Application	ibm	Db2	9.0	All	All	All
Application	ibm	Db2	9.0	fp1	All	All
Application	ibm	Db2	8.2	All	All	All
Application	ibm	Db2	8.2	fp1	All	All
Application	ibm	Db2	8.2	fp2	All	All
Application	ibm	Db2	8.2	fp3	All	All
Application	ibm	Db2	8.2	fp4	All	All
Application	ibm	Db2	8.2	fp5	All	All
Application	ibm	Db2	8.2	fp6	All	All
Application	ibm	Db2	9.0	All	All	All

Application	Ibm	Db2	9.0	fp1	All	All
Operating System	Unix	Unix	All	All	All	All
Operating System	Unix	Unix	All	All	All	All

References

Reference	Source	Link	Ta
IBM DB2 Fenced UserID Directory Access Authentication Bypass - Advisories - Secunia	SECUNIA	secunia.com	Ve
IBM DB2 Local Fenced Processes Can Access Restricted Directories - SecurityTracker	SECTRAK	www.securitytracker.com	
IBM DB2 Fenced UserID Unspecified Authentication Bypass Vulnerability	BID	www.securityfocus.com	
IY87492: SECURITY: FENCED USERID INCORRECTLY ABLE TO ACCESS DIRECTORIES	AIXAPAR	www-1.ibm.com	Ve
IBM notice: The page you requested cannot be displayed	AIXAPAR	www-1.ibm.com	Ve
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca



No vendor comments have been submitted for this CVE.

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