

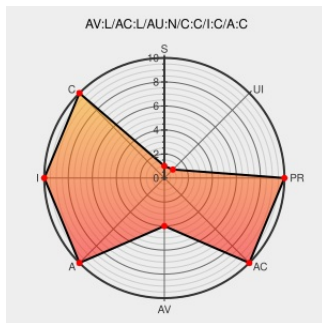


CVE-2003-1052

Published on: 08/20/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1052

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

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

IBM DB2 7.1 and 8.1 allow the bin user to gain root privileges by modifying the shared libraries that are used in setuid root programs.

CVE-2003-1052 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

IBM DB2 Shared Library Injection
Vulnerability

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 8346](#)

SecurityFocus HOME Mailing List:
BugTraq

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[www.securityfocus.com](#)
[text/html](#)

[🌐](#) [BUGTRAQ 20030805 Slight privilege elevation from bin to root in IBM DB2 7.1 - 8.1 all binaries](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[🔑](#) [XF ibm-db2-gain-privileges\(12826\)](#)

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

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	lbn	Db2	9.0	All	All	All
Application	lbn	Db2	9.0	All	All	All
Application	lbn	Db2 Universal Database	6.0	All	All	All
Application	lbn	Db2 Universal Database	7.0	All	linux	All
Application	lbn	Db2 Universal Database	7.1	All	linux	All
Application	lbn	Db2 Universal Database	7.2	All	linux	All
Application	lbn	Db2 Universal Database	8.0	All	linux	All
Application	lbn	Db2 Universal Database	8.1	All	aix	All
Application	lbn	Db2 Universal Database	8.2	All	windows	All
Application	lbn	Db2 Universal Database	6.0	All	All	All
Application	lbn	Db2 Universal Database	7.0	All	linux	All
Application	lbn	Db2 Universal Database	7.1	All	linux	All
Application	lbn	Db2 Universal Database	7.2	All	linux	All
Application	lbn	Db2 Universal Database	8.0	All	linux	All
Application	lbn	Db2 Universal Database	8.1	All	aix	All
Application	lbn	Db2 Universal Database	8.2	All	windows	All

```
cpe:2.3:a:ibm:db2:9.0:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:db2:9.0:*:*:*:*:*:*:
```

cpe:2.3:a:ibm:db2_universal_database:6.0.*:*:*:*:*:

```
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:8.0:*:linux:*:*:*:*:*
```

```
cpe:2.3:a:ibm:db2_universal_database:8.1:*:aix:*:*:*:*:
```

```
cpe:2.3:a:ibm:db2_universal_database:8.2.*:windows:*:*:*:*.*
```

```
cpe:2.3:a:ibm:db2_universal_database:6.0.*:*:*:*:*:*
```

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:8.0:*:linux:*:*:*:*:
cpe:2.3:a:ibm:db2_universal_database:8.1:*:aix:*:*:*:*:
cpe:2.3:a:ibm:db2_universal_database:8.2:*:windows:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)