CVE-2014-6159

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-6159
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-08 11:55:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	IBM DB2 9.7 before FP10, 9.8 through FP5, 10.1 through FT4, and 10.5 through FP4 on Linux, UNIX, and Windows, when

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Db2	10.1	All	All	All
Application	Ibm	Db2	10.5	All	All	All
Application	Ibm	Db2	9.7	All	All	All
Application	Ibm	Db2	9.8	All	All	All
Application	Ibm	Db2	10.1	All	All	All
Application	Ibm	Db2	10.5	All	All	All
Application	Ibm	Db2	9.7	All	All	All
Application	Ibm	Db2	9.8	All	All	All

References

Reference
IBM Security Bulletin: IBM® DB2® LUW contains a vulnerability in which an ALTER TABLE statement may cause the DB2 server to terminate
IT05105: SECURITY: DB2 may terminate abnormally when issuing an ALTER TAB LE statement with AUTO_REVAL set to IMMEDIATE (CVE
Security Advisory SA62093 - IBM DB2 / DB2 Connect Multiple Denial of Service Vulnerabilities - Secunia
Security Advisory SA62092 - IBM InfoSphere BigInsights Security Issue and Multiple Vulnerabilities - Secunia
IBM IT05074: SECURITY: DB2 may terminate abnormally when issuing an ALTER TAB LE statement with AUTO_REVAL set to IMMEDIATE
IBM IT04730: SECURITY: DB2 may terminate abnormally when issuing an ALTER TAB LE statement with AUTO_REVAL set to IMMEDIATE

IT05132
Multiple IBM DB2 Products CVE-2014-6159 Remote Denial of Service Vulnerability
Security Bulletin: Infosphere BigInsights contains multiple vulnerabilities in which an ALTER TABLE statement may cause the Big SQL server
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**