



CVE-2023-27868

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

Summary

CVE	CVE-2023-27868
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-10 16:15:00 UTC
Updated	2023-08-03 15:15:00 UTC
Description	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attack

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Application	Ibm	Db2	10.5.0.11	All	All	All
Application	Ibm	Db2	11.1.4.7	All	All	All
Application	Ibm	Db2	11.5	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Oracle	Solaris	-	All	All	All

References

Reference
IBM X-Force Exchange
July 2023 IBM DB2 JDBC Driver Vulnerabilities in NetApp Products NetApp Product Security
Security Bulletin: IBM® Db2® JDBC driver is vulnerable to remote code execution. (CVE-2023-27869, CVE-2023-27867, CVE-2023-27868)
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[20352](#) IBM Db2 Multiple Remote Code Execution (RCE) Vulnerabilities (7010029)

© [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](#)