



CVE-2018-1897

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

Summary

CVE	CVE-2018-1897
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-30 15:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	IBM DB2 for Linux, UNIX and Windows 9.7, 10.1, 10.5., and 11.1 db2pdcfg is vulnerable to a stack based buffer overflow, c

Risk And Classification

Problem Types: CWE-787

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	11.1	All	All	All
Application	ibm	Db2	9.7	All	All	All
Application	ibm	Db2	10.1	All	All	All
Application	ibm	Db2	10.5	All	All	All
Application	ibm	Db2	11.1	All	All	All
Application	ibm	Db2	9.7	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link
IBM DB2 'db2pdcfg' CVE-2018-1897 Local Buffer Overflow Vulnerability	BID	www.securi
IBM DB2 Buffer Overflow in 'db2pdcfg' Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.securi

IBM X-Force Exchange	XF	exchange.x
Security Bulletin: IBM® Db2® is vulnerable to a buffer overflow leading to privilege escalation (CVE-2018-1897).	CONFIRM	www.ibm.cc
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)