



CVE-2014-4981

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-4981
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-17 22:15:00 UTC
Updated	2020-02-20 16:15:00 UTC
Description	LPAR2RRD in 3.5 and earlier allows remote attackers to execute arbitrary commands due to insufficient input sanitization o

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xorux	Lpar2rrd	All	All	All	All

References

Reference	Source	Link	Tags
LPAR2RRD 3.5 / 4.53 Command Injection ~ Packet Storm	MISC	packetstormsecurity.com	Third Party Adviso
oss-security - [oCERT-2014-005] LPAR2RRD input sanitization errors	MISC	www.openwall.com	Mailing List, Third
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	Third Party Adviso
oCERT.org - oCERT Advisories	MISC	ocert.org	Third Party Adviso
AIX / IBM i monitoring and capacity planning : LPAR2RRD	MISC	www.lpar2rrd.com	Vendor Advisory
LPAR2RRD CVE-2014-4981 Unspecified Command Injection Vulnerability	BID	www.securityfocus.com	Third Party Adviso
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

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](#)