



CVE-2018-1724

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

Summary

CVE	CVE-2018-1724
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-11 12:29:00 UTC
Updated	2019-10-09 23:38:00 UTC
Description	IBM Spectrum LSF 9.1.1 9.1.2, 9.1.3, and 10.1 could allow a local user to change their job user at job submission time due

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Spectrum Lsf	10.1	All	All	All
Application	ibm	Spectrum Lsf	9.1.1	All	All	All
Application	ibm	Spectrum Lsf	9.1.2	All	All	All
Application	ibm	Spectrum Lsf	9.1.3	All	All	All
Application	ibm	Spectrum Lsf	10.1	All	All	All
Application	ibm	Spectrum Lsf	9.1.1	All	All	All
Application	ibm	Spectrum Lsf	9.1.2	All	All	All
Application	ibm	Spectrum Lsf	9.1.3	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	VDB E
Security Bulletin: IBM Spectrum LSF is affected by a privilege escalation vulnerability	CONFIRM	www-01.ibm.com	Mitigat
IBM Spectrum LSF CVE-2018-1724 Local Security Bypass Vulnerability	BID	www.securityfocus.com	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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](#)