



CVE-2021-29751

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

Summary

CVE	CVE-2021-29751
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-28 16:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 could allow an a

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Business Automation Workflow	18.0.0.0	All	All	All
Application	ibm	Business Automation Workflow	19.0.0.0	All	All	All
Application	ibm	Business Automation Workflow	20.0.0.0	All	All	All
Application	ibm	Business Process Manager	8.5.0.0	All	All	All
Application	ibm	Business Process Manager	8.6.0.0	All	All	All

References

Reference	Source	Link
Security Bulletin: Incorrect authorization in IBM Business Automation Workflow and IBM Business Process Manager (BPM)	CONFIRM	ww
Security Bulletin: Multiple vulnerabilities affect IBM Cloud Pak for Automation	CONFIRM	ww
IBM X-Force Exchange	XF	ex
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

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](#)