



# CVE-2020-4794

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-4794
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@us.ibm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-21 18:15:00 UTC
<b>Updated</b>	2020-12-22 16:28:00 UTC
<b>Description</b>	IBM Automation Workstream Services 19.0.3, 20.0.1, 20.0.2, IBM Business Automation Workflow 18.0, 19.0, and 20.0 and

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Automation Workstream Services	19.0.3	All	All	All
Application	ibm	Automation Workstream Services	20.0.1	All	All	All
Application	ibm	Automation Workstream Services	20.0.2	All	All	All
Application	ibm	Automation Workstream Services	19.0.3	All	All	All
Application	ibm	Automation Workstream Services	20.0.1	All	All	All
Application	ibm	Automation Workstream Services	20.0.2	All	All	All
Application	ibm	Business Automation Workflow	18.0.0.0	All	All	All
Application	ibm	Business Automation Workflow	18.0.0.1	All	All	All
Application	ibm	Business Automation Workflow	18.0.0.2	All	All	All
Application	ibm	Business Automation Workflow	19.0.0.0	All	All	All
Application	ibm	Business Automation Workflow	19.0.0.1	All	All	All
Application	ibm	Business Automation Workflow	19.0.0.2	All	All	All
Application	ibm	Business Automation Workflow	19.0.0.3	All	All	All
Application	ibm	Business Automation Workflow	20.0.0.0	All	All	All
Application	ibm	Business Automation Workflow	20.0.0.1	All	All	All
Application	ibm	Business Automation Workflow	20.0.2.0	All	All	All
Application	ibm	Business Automation Workflow	18.0.0.0	All	All	All





Application	ibm	<a href="#">Business Process Manager</a>	8.5.6.2	All	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	All	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	All	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201606	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201606	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201609	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201609	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201612	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201612	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201703	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201703	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201706	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.5.7.0	cf201706	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.6	All	All	All
Application	ibm	<a href="#">Business Process Manager</a>	8.6	All	All	All

## References

### Reference

IBM X-Force Exchange

Security Bulletin: Information disclosure and Denial of Service vulnerability affect IBM Business Automation Workflow and IBM Business Process Manager

CVE Program record

NVD vulnerability detail

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](#)