



CVE-2021-29872

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

Summary

CVE	CVE-2021-29872
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-18 17:15:00 UTC
Updated	2022-01-25 16:29:00 UTC
Description	IBM Cloud Pak for Automation 21.0.1 and 21.0.2 - Business Automation Studio Component is vulnerable to HTTP header in

Risk And Classification

Problem Types: CWE-116

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Cloud Pak For Automation	All	All	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	All	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	interim_fix001	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	interim_fix002	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	interim_fix003	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	interim_fix004	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	interim_fix005	All	All
Application	ibm	Cloud Pak For Automation	21.0.1	interim_fix006	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	All	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	interim_fix001	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	interim_fix002	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	interim_fix003	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	interim_fix004	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	interim_fix005	All	All
Application	ibm	Cloud Pak For Automation	21.0.2	interim_fix006	All	All

References

Reference	Source
IBM X-Force Exchange	XF
Security Bulletin: Host header injection vulnerability in Business Automation Studio in Cloud Pak for Automation (CVE-2021-29872)	CONFIR
CVE Program record	CVE.O
NVD vulnerability detail	NVD

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](#)