



CVE-2021-38966

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

Summary

CVE	CVE-2021-38966
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-21 19:15:00 UTC
Updated	2021-12-23 19:43:00 UTC
Description	IBM Cloud Pak for Automation 21.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Cloud Pak For Automation	21.0.2	-	All	All
Application	ibm	Workflow Process Service	21.0.2	All	All	All

References

Reference

Security Bulletin: Cross-Site Scripting vulnerability affect IBM Cloud Pak for Automation Workflow Process Service (CVE-2021-38893 CVE-20

IBM X-Force Exchange

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.

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