



CVE-2022-46773

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

Summary

CVE	CVE-2022-46773
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-15 20:15:00 UTC
Updated	2023-11-07 03:55:00 UTC
Description	IBM Robotic Process Automation 21.0.0 - 21.0.7 and 23.0.0 is vulnerable to client-side validation bypass for credential pool

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Robotic Process Automation	All	All	All	All
Application	Ibm	Robotic Process Automation	23.0.0	All	All	All
Application	Ibm	Robotic Process Automation As A Service	All	All	All	All
Application	Ibm	Robotic Process Automation For Cloud Pak	All	All	All	All
Application	Ibm	Robotic Process Automation For Cloud Pak	23.0.0	All	All	All

References

Reference
Security Bulletin: A vulnerability in IBM Robotic Process Automation may allow a user to create invalid credential pools (CVE-2022-46773)
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.

© [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](#)