



# CVE-2022-22412

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2022-22412   |
| <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>       | 2022-07-26 15:15:00 UTC  |
| <b>Updated</b>         | 2022-08-02 18:55:00 UTC  |
| <b>Description</b>     | IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with access to the local host (client machine |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor    | Product                    | Version | Update | Edition | Language |
|------------------|-----------|----------------------------|---------|--------|---------|----------|
| Application      | IBM       | Robotic Process Automation | All     | All    | All     | All      |
| Operating System | Microsoft | Windows                    | -       | All    | All     | All      |

## References

| Reference  | Source  | L |
|--|---------|---|
| IBM X-Force Exchange   | XF      | e |
| Security Bulletin: IBM Robotic Process Automation is vulnerable to insufficiently protected access tokens (CVE-2022-22412) | CONFIRM | w |
| CVE Program record   | CVE.ORG | w |
| NVD vulnerability detail   | NVD     | n |

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**