Severity

Medium

Analysis Summary

CVE-2022-22434 CVSS:4.2

IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with physical access to create an API request modified to create additional objects.

CVE-2022-22433 CVSS:2.7

IBM Robotic Process Automation 21.0.1 and 21.0.2 is vulnerable to External Service Interaction attack, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to induce the application to perform server-side DNS lookups or HTTP requests to arbitrary domain names. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with.

CVE-2022-22415 CVSS:4.3

A vulnerability exists where an IBM Robotic Process Automation 21.0.1 regular user is able to obtain view-only access to some admin pages in the Control Center

CVE-2021-39020 CVSS:2

IBM Guardium Data Encryption (GDE) 4.0.0.7 and lower stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history.

Impact

- Data Manipulation
- Security Bypass
- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-22434
- CVE-2022-22433
- CVE-2022-22415
- CVE-2021-39020

Affected Vendors

- IBM

Affected Products

- IBM Robotic Process Automation 21.0.0
- IBM Robotic Process Automation 21.0.1
- IBM Robotic Process Automation 21.0.2
- IBM Guardium Data Encryption 4.0.0
- IBM Guardium Data Encryption 5.0.0

Remediation

Refer to IBM Security Bulletin for patch, upgrade or suggested workaround information.

IBM Security Bulletin (Robotic Process Automation)

IBM Security Bulletin (Guardium Data Encryption)