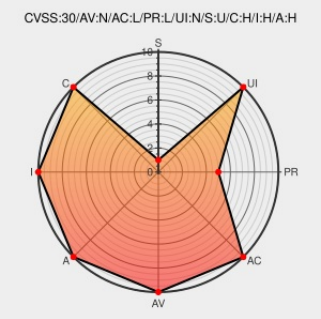
CVE-2019-11875

Published on: 05/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:36 PM UTC

CVE-2019-11875

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Robotic Process Automation from Blueprism contain the following vulnerability:

In AutomateAppCore.dll in Blue Prism Robotic Process Automation 6.4.0.8445, a vulnerability in access control can be exploited to escalate privileges. The vulnerability allows for abusing the application for fraud or unauthorized access to certain information. The attack requires a valid user account to connect to the Blue Prism server, but the roles associated to this account are not required to have any permissions. First of all, the application files are modified to grant full permissions on the client side. In a test environment (or his own instance of the software) an attacker is able to grant himself full privileges also on the server side. He can then, for instance, create a process with malicious behavior and export it to disk. With the modified client, it is possible to import the exported file as a release and overwrite any existing process in the database. Eventually, the bots execute the malicious process. The server does not check the user's permissions for the aforementioned actions, such that a modification of the client software enables this kind of attack. Possible scenarios may involve changing bank accounts or setting passwords.

CVE-2019-11875 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Exploit Third Party Advisory www.syss.de text/plain	MISC www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-002.txt
Blue Prism Robotic Process Automation (RPA) Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153007/Blue-Prism-Robotic-Process-Automation-RPA-Privilege-Escalation.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

375722 Blue Prism Robotic Process Automation (RPA) Privilege Escalation Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Blueprism	Robotic Process Automation	6.4.0.8445	All	All	All
Application	Blueprism	Robotic Process Automation	6.4.0.8445	All	All	All

cpe:2.3:a:blueprism:robotic_process_automation:6.4.0.8445:*:*:*:*:*:*:*:

cpe:2.3:a:blueprism:robotic_process_automation:6.4.0.8445:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→