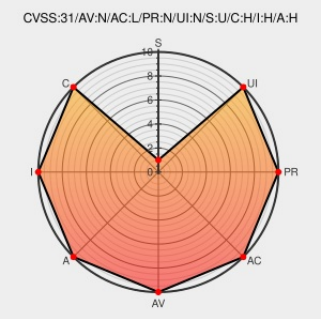
CVE-2020-9423

Published on: 03/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:15 PM UTC

CVE-2020-9423

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



Certain versions of Logicaldoc from Logicaldoc contain the following vulnerability:

LogicalDoc before 8.3.3 could allow an attacker to upload arbitrary files, leading to command execution or retrieval of data from the database. LogicalDoc provides a functionality to add documents. Those documents could then be used for multiple tasks, such as version control, shared among users, applying tags, etc. This functionality could be abused by an unauthenticated attacker to upload an arbitrary file in a restricted folder. This would lead to the executions of malicious commands with root privileges.

CVE-2020-9423 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

LogicalDoc Virtual Appliance Multiple Vulnerabilities	Exploit Third Party Advisory www.coresecurity.com text/html	MISC www.coresecurity.com/advisories/logicaldoc-virtual-appliance-multiple-vulnerabilities

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Logicaldoc	Logicaldoc	All	All	All	All
Application	Logicaldoc	Logicaldoc	All	All	All	All

cpe:2.3:a:logicaldoc:logicaldoc:*:*:*:*:*:*:*:*:

cpe:2.3:a:logicaldoc:logicaldoc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→