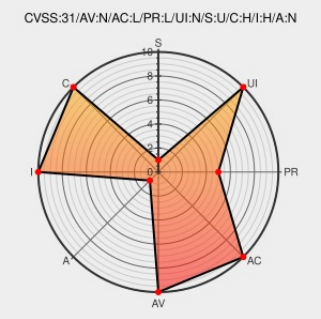
CVE-2020-24985

Published on: 03/15/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-24985

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



Certain versions of Espressdashboard from Quadbase contain the following vulnerability:

An issue was discovered in Quadbase EspressReports ES 7 Update 9. An authenticated user is able to navigate to the MenuPage section of the application, and change the frmsrc parameter value to retrieve and execute external files or payloads.

CVE-2020-24985 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2020-24985 – C41NC	c41nc.co.uk text/html	MISC c41nc.co.uk/cve-2020-24985/

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	Quadbase	Espressdashboard	7.0	update9	All	All
Application	Quadbase	Expressdashboard	7.0	update9	All	All

cpe:2.3:a:quadbase:espressdashboard:7.0:update9:*:*:*:*:*:*:

cpe:2.3:a:quadbase:expressdashboard:7.0:update9:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→