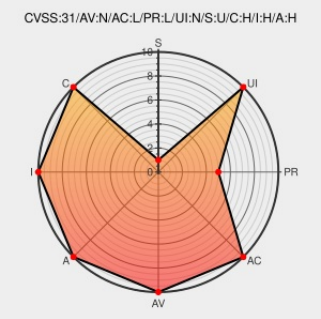
CVE-2020-10382

Published on: 04/14/2020 12:00:00 AM UTC

Last Modified on: 11/21/2022 08:13:00 PM UTC

CVE-2020-10382

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



Certain versions of Mbconnect24 from Mbconnectline contain the following vulnerability:

An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an authenticated remote code execution in the backup-scheduler.

CVE-2020-10382 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
Security Advice - MB connect line GmbH	mbconnectline.com text/html	CONFIRM mbconnectline.com/security-advice/

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	Mbconnectline	Mbconnect24	All	All	All	All
Application	Mbconnectline	Mymbconnect24	All	All	All	All

cpe:2.3:a:mbconnectline:mbconnect24:*:*:*:*:*:*:*:*:

cpe:2.3:a:mbconnectline:mymbconnect24:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→