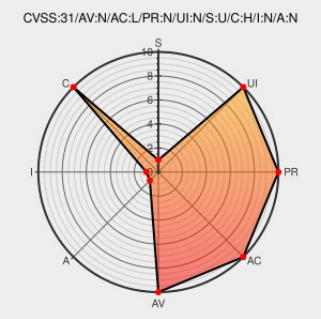
CVE-2020-25966

Published on: 10/28/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:20:00 AM UTC

CVE-2020-25966

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



Certain versions of Spectra from Sectona contain the following vulnerability:

** DISPUTED ** Sectona Spectra before 3.4.0 has a vulnerable SOAP API endpoint that leaks sensitive information about the configured assets without proper authentication. This could be used by unauthorized parties to get configured login credentials of the assets via a modified pAccountID value. NOTE: The vendor has indicated this is not a vulnerability and states "This vulnerability occurred due to wrong configuration of system."

CVE-2020-25966 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Mohamed Gazzaz / Sectona PAM API Issue	Exploit	MISC gitlab.com/Gazzaz/Spectra_API_Issue/

Mohamed Gazzaz / Sectona_PAM_API_Issue · GitLab	Exploit Third Party Advisory gitlab.com text/html	MISC gitlab.com/Gazzaz/Spectra_API_Issue/
Spectra Privileged Access Management - Sectona	Product web.archive.org text/html Inactive Link Not Archived	MISC sectona.com/products/spectra-privileged-access-management/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sectona	Spectra	All	All	All	All
Application	Sectona	Spectra	All	All	All	All

cpe:2.3:a:sectona:spectra:*:*:*:*:*:*:*:*:

cpe:2.3:a:sectona:spectra:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→