

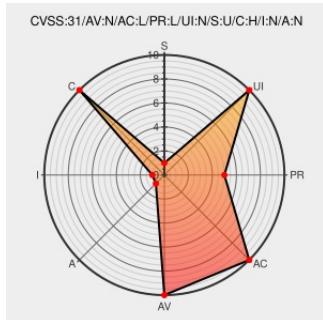


CVE-2020-25130

Published on: 09/25/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:31 PM UTC

CVE-2020-25130

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Observium](#) from [Observium](#) contain the following vulnerability:

An issue was discovered in Observium Professional, Enterprise & Community 20.8.10631. It is vulnerable to SQL Injection due to the fact that it is possible to inject malicious SQL statements in malformed parameter types. Sending an improper variable type of Array allows a bypass of core SQL Injection sanitization. Authenticated users are able

to inject malicious SQL queries. This vulnerability leads to full database leak including ckeys that can be used in the authentication process without knowing the username and cleartext password. This can occur via the ajax/actions.php group_id field.

CVE-2020-25130 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Exploit

Third Party Advisory

gist.github.com

text/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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Observium	Observium	20.8.10631	All	All	All
Application	Observium	Observium	20.8.10631	All	All	All
Application	Observium	Observium	20.8.10631	All	All	All
Application	Observium	Observium	20.8.10631	All	All	All
Application	Observium	Observium	20.8.10631	All	All	All
Application	Observium	Observium	20.8.10631	All	All	All
cpe:2.3:a:observium:observium:20.8.10631:*:*:*:community:*:*:						
cpe:2.3:a:observium:observium:20.8.10631:*:*:*:enterprise:*:*:						
cpe:2.3:a:observium:observium:20.8.10631:*:*:*:professional:*:*:						
cpe:2.3:a:observium:observium:20.8.10631:*:*:*:community:*:*:						
cpe:2.3:a:observium:observium:20.8.10631:*:*:*:enterprise:*:*:						
cpe:2.3:a:observium:observium:20.8.10631:*:*:*:professional:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →