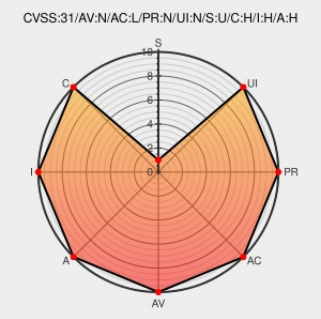
CVE-2020-25132

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

Last Modified on: 03/23/2021 11:23:32 PM UTC

CVE-2020-25132

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 the improper variable type Array allows a bypass of core SQL Injection sanitization. Users are able to inject malicious statements in multiple functions. This vulnerability leads to full authentication bypass: any unauthorized user with access to the application is able to exploit this vulnerability. This can occur via the Cookie header to the default URI, within includes/authenticate.inc.php.

CVE-2020-25132 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: 7.5 - HIGH

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

CVE References

Description	Tags	Link
CVE-2020-25132 · GitHub	Exploit Third Party Advisory gist.github.com text/html	MISC gist.github.com/mariuszpoplawski/e70bc0afe5853e283d3fd3511a1ce09d

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report