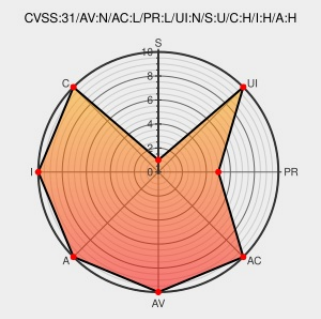
CVE-2020-25134

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

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

CVE-2020-25134

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 directory traversal and local file inclusion due to the fact that there is an unrestricted possibility of loading any file with an inc.php extension. Inclusion of other files (even though limited to the mentioned extension) can lead to Remote Code Execution. This can occur via /settings/?format=../ URIs to pages/settings.inc.php.

CVE-2020-25134 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
CVE-2020-25134 · GitHub	Third Party Advisory gist.github.com	MISC gist.github.com/mariuszpoplawski/a3d18fc3d7113cf9c004161ebd9420c9

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

Exploit/POC from Github

CVE-2020-25134 Authenticated Local File Inclusion in settings/format

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→