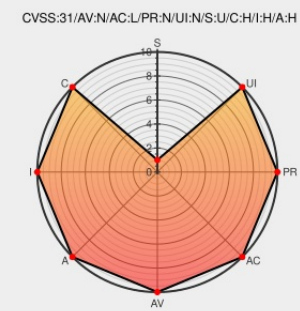
CVE-2023-35189

Published on: Not Yet Published

Last Modified on: 07/27/2023 05:43:00 PM UTC

CVE-2023-35189

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



Certain versions of Scrutisweb from Iagona contain the following vulnerability:

Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a remote code execution vulnerability that could allow an unauthenticated user to upload a malicious payload and execute it.

CVE-2023-35189 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **iagona** - **ScrutisWeb** version **<= 2.1.37**

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

CVE References

Description	Tags	Link
Iagona ScrutisWeb | CISA	www.cisa.gov text/html	MISC www.cisa.gov/news-events/ics-advisories/icsa-23-199-03

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	Iagona	Scrutisweb	All	All	All	All

cpe:2.3:a:iagona:scrutisweb:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→