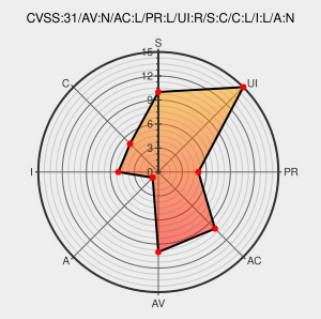
CVE-2021-40610

Published on: Not Yet Published

Last Modified on: 06/15/2022 04:18:00 PM UTC

CVE-2021-40610

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



Certain versions of Emlog Pro from Emlog Pro Project contain the following vulnerability:

Emlog Pro v 1.0.4 cross-site scripting (XSS) in Emlog Pro background management.

CVE-2021-40610 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
emlog pro v 1.0.4 management XSS Vulnerability · Issue #1 · blackQvQ/emlog · GitHub	github.com text/html	MISC github.com/blackQvQ/emlog/issues/1

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	Emlog Pro Project	Emlog Pro	1.0.4	All	All	All

cpe:2.3:a:emlog_pro_project:emlog_pro:1.0.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40610 : Emlog Pro v 1.0.4 cross-site scripting #XSS in Emlog Pro background management.... cve.report/CVE-2021-40610	2022-06-09 13:05:17
/r/netcve	CVE-2021-40610	2022-06-09 13:38:18

← Previous ID

Next ID→