

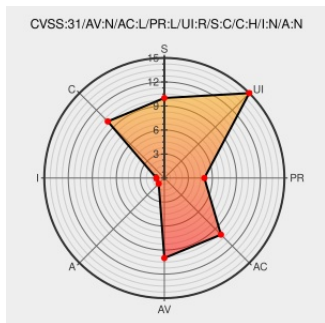


CVE-2021-41156

Published on: 10/18/2021 12:00:00 AM UTC

Last Modified on: 10/22/2021 04:15:00 PM UTC

CVE-2021-41156 - advisory for GHSA-g9cc-m4p4-6xpc

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

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

anuko/timetracker is an, open source time tracking system. In affected versions Time Tracker uses browser_today hidden control on a few pages to collect the today's date from user browsers. Because of not checking this parameter for sanity in versions prior to 1.19.30.5601, it was possible to craft an html form with malicious JavaScript, use social

engineering to convince logged on users to execute a POST from such form, and have the attacker-supplied JavaScript to be executed in user's browser. This has been patched in version 1.19.30.5600. Upgrade is recommended. If it is not practical, introduce ttValidDbDateFormatDate function as in the latest version and add a call to it within the access checks block.

CVE-2021-41156 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **anuko** - **timetracker** version < 1.19.30.5601

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
Reflected XSS vulnerability · Advisory · anuko/timetracker · GitHub	github.com text/html	CONFIRM github.com/anuko/timetracker/security/advisories/GHSA-g9cc-m4p4-6xpc

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	Timetracker Project	Timetracker	All	All	All	All

cpe:2.3:a:timetracker_project:timetracker:*:*:*:*:*.*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41156 : anuko/timetracker is an, open source time tracking system. In affected versions Time Tracker uses... twitter.com/i/web/status/1...	2021-10-18 21:15:26

← Previous ID

Next ID →