



CVE-2021-41139

Published on: 10/13/2021 12:00:00 AM UTC

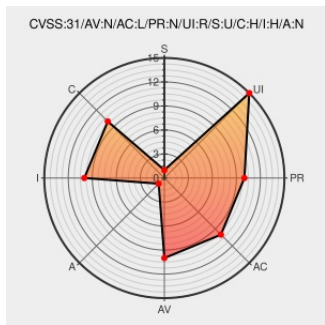
Last Modified on: 10/20/2021 07:17:00 PM UTC

CVE-2021-41139 - advisory for GHSA-h2v8-87c9-86cw

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Time Tracker](#) from [Anuko](#) contain the following vulnerability:

Anuko Time Tracker is an open source, web-based time tracking application written in PHP. When a logged on user selects a date in Time Tracker, it is being passed on via the date parameter in URI. Because of not checking this parameter for sanity in versions prior to 1.19.30.5600, it was possible to craft the URI with malicious

JavaScript, use social engineering to convince logged on user to click on such link, and have the attacker-supplied JavaScript to be executed in user's browser. This issue is patched in version 1.19.30.5600. As a workaround, one may introduce `ttValidDbDateFormatDate` function as in the latest version and add a call to it within the access checks block in time.php.

CVE-2021-41139 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **anuko - timetracker** version < 1.19.30.5600

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Added a check for passed in date to time.php. · anuko/timetracker@5599067 · GitHub	github.com text/html	MISC github.com/anuko/timetracker/commit/559906731f153c9b3a632c2839ed11669b76d593
Reflected XSS vulnerability in time.php · Advisory · anuko/timetracker · GitHub	github.com text/html	CONFIRM github.com/anuko/timetracker/security/advisories/GHSA-h2v8-87c9-86cw
A better fix to validate a passed-in date. · anuko/timetracker@d3f60bd · GitHub	github.com text/html	MISC github.com/anuko/timetracker/commit/d3f60bd3e3ea8ff8ec31a596baec6750af601b7c

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	Anuko	Time Tracker	All	All	All	All
<code>cpe:2.3:a:anuko:time_tracker:*.:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41139 : Anuko Time Tracker is an open source, web-based time tracking application written in PHP. When a l... twitter.com/i/web/status/1...	2021-10-13 17:14:56

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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