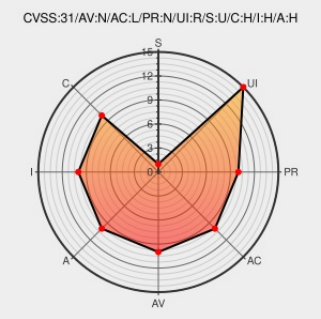
CVE-2022-31149

Published on: Not Yet Published

Last Modified on: 09/13/2022 10:45:00 PM UTC

CVE-2022-31149 - advisory for GHSA-v9fg-6g9j-h4x4

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



Certain versions of Activitywatch from Activitywatch contain the following vulnerability:

ActivityWatch open-source automated time tracker. Versions prior to 0.12.0b2 are vulnerable to DNS rebinding attacks. This vulnerability impacts everyone running ActivityWatch and gives the attacker full access to the ActivityWatch REST API. Users should upgrade to v0.12.0b2 or later to receive a patch. As a workaround, block DNS lookups that resolve to 127.0.0.1.

CVE-2022-31149 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **ActivityWatch** - **activitywatch** version **< 0.12.0b2**

CVSS3 Score: 9.6 - CRITICAL

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

CVE References

Description	Tags	Link
ActivityWatch disclosure · GitHub	gist.github.com text/html	MISC gist.github.com/zozs/fdebbce75fc8538c15851b46db944a16
v0.12.0 · Discussion #778 · ActivityWatch/activitywatch · GitHub	github.com text/html	MISC github.com/ActivityWatch/activitywatch/discussions/778
DNS rebinding attack · Advisory · ActivityWatch/activitywatch · GitHub	github.com text/html	CONFIRM github.com/ActivityWatch/activitywatch/security/advisories/GHSA-v9fg-6g9j-h4x4

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	Activitywatch	Activitywatch	All	All	All	All
Application	Activitywatch	Activitywatch	0.12.0	beta1	All	All

cpe:2.3:a:activitywatch:activitywatch:*:*:*:*:*:*:*:*:

cpe:2.3:a:activitywatch:activitywatch:0.12.0:beta1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31149 : ActivityWatch open-source automated time tracker. Versions prior to 0.12.0b2 are vulnerable to DNS… twitter.com/i/web/status/1…	2022-09-07 13:53:02
/r/netcve	CVE-2022-31149	2022-09-07 14:38:52

← Previous ID

Next ID→