



CVE-2022-23949

Published on: Not Yet Published

Last Modified on: 09/22/2022 04:22:00 PM UTC

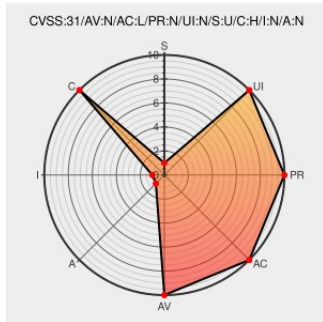
CVE-2022-23949

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In Keylime before 6.3.0, unsanitized UUIDs can be passed by a rogue agent and can lead to log spoofing on the verifier and registrar.

CVE-2022-23949 has been assigned by patrick@puiterwijk.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
validators: create validators module · keylime/keylime@65c2b73 · GitHub	github.com text/html	MISC github.com/keylime/keylime/commit/65c2b737129b5837f4a03660aeb1191ced275a57
validators: add uuid and agent_id validators · keylime/keylime@e429e95 · GitHub	github.com text/html	MISC github.com/keylime/keylime/commit/e429e95329fc60608713ddfb82f4a92ee3b3d2d9
Validate user ID in all public interfaces · keylime/keylime@387e320 · GitHub	github.com text/html	MISC github.com/keylime/keylime/commit/387e320dc22c89f4f47c68cb37eb9eec2137f34b
oss-sec: keylime: Multiple Security Issues (including remote code execution in the Agent component)	seclists.org text/html	MISC seclists.org/oss-sec/2022/q1/101
Keylime: Unsanitized UUIDs can lead to log spoofing · Advisory ·	github.com text/html	MISC github.com/keylime/keylime/security/advisories/GHSA-87gh-qc28-j9mm

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.

Related QID Numbers

[282323](#) Fedora Security Update for keylime (FEDORA-2022-dbb274913a)



[282324](#) Fedora Security Update for keylime (FEDORA-2022-5770dad5f8)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Keylime	Keylime	All	All	All	All
cpe:2.3:a:keylime:keylime:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-23949 : In Keylime before 6.3.0, unsanitized UUIDs can be passed by a rogue agent and can lead to log spoo... twitter.com/i/web/status/1...	2022-09-21 19:06:34
 /r/netcve	CVE-2022-23949	2022-09-21 20:38:45

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022   |

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](#)