



CVE-2022-23950

Published on: Not Yet Published

Last Modified on: 09/22/2022 04:21:00 PM UTC

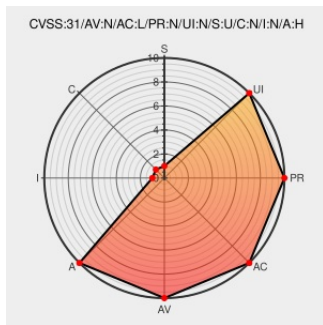
CVE-2022-23950

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **Keylime** from **Keylime** contain the following vulnerability:

In Keylime before 6.3.0, Revocation Notifier uses a fixed /tmp path for UNIX domain socket which can allow unprivileged users a method to prohibit keylime operations.

CVE-2022-23950 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	NONE	NONE	HIGH

CVE References

Description	Tags	Link
revocation_notifier: move zmq socket to /var/run/keylime · keylime/keylime@ea5d037 · GitHub	github.com text/html	MISC github.com/keylime/keylime/commit/ea5d0373fa2c050d5d95404eb779be7e8327b911
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: Revocation Notifier's UNIX unprivileged domain socket which can allow DOS · Advisory · keylime/keylime · GitHub	github.com text/html	MISC github.com/keylime/keylime/security/advisories/GHSA-9r9r-f8xc-m875

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

CVE.report 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
<code>cpe:2.3:a:keylime:keylime:*:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-23950 : In Keylime before 6.3.0, Revocation Notifier uses a fixed /tmp path for UNIX domain socket which c... twitter.com/i/web/status/1...	2022-09-21 19:06:53
 /r/netcve	CVE-2022-23950	2022-09-21 20:38:46

[← 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](#)