



# CVE-2022-28352

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2022-28352
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-02 17:15:00 UTC
<b>Updated</b>	2022-04-13 18:33:00 UTC
<b>Description</b>	WeeChat (aka Wee Enhanced Environment for Chat) 3.2 to 3.4 before 3.4.1 does not properly verify the TLS certificate of t

## Risk And Classification

**Problem Types:** CWE-295

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Weechat	Weechat	All	All	All	All

## References

Reference	Source
WeeChat :: documentation :: security	MISC
Having to re-set the weechat.network.gnutls_ca_user env variable every single session. · Issue #1763 · weechat/weechat · GitHub	MISC
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[184045](#) Debian Security Update for weechat (CVE-2022-28352)

[502200](#) Alpine Linux Security Update for weechat

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](#)**