

[Stable](#) [Development](#) [Old versions](#) [Security](#)

[All vulnerabilities](#) [Vulnerabilities by version](#)

Overview: 1 vulnerability

WSA	CVE	Score	Severity	Issue	Vulnerability type	Scope	Versions	Fix
WSA-2022-1	CVE-2022-28352	4.3		Possible man-in-the-middle attack in TLS connection to servers.	Improper certificate validation	IRC, Plugins	3.2 → 3.4	3.4.1



[WSA-2022-1](#): [IRC, Plugins] Possible man-in-the-middle attack in TLS connection to servers.

Vulnerability

CVE

CVE-2022-28352 [[MITRE](#) / [NVD](#)]

CVSS vector

AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N ([detail](#))

CVSS score

4.3 / 10

Severity

medium

Vulnerability type

Improper certificate validation ([detail](#))

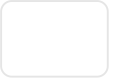
Scope

IRC, Plugins

Affected versions

3.2 → 3.4

Fixed version



Description

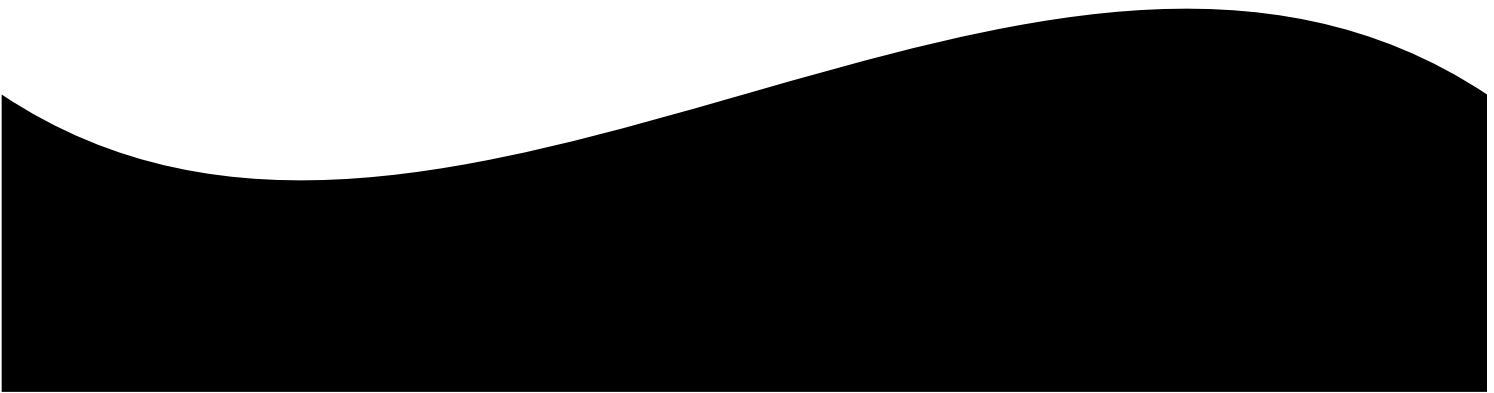
After changing the options `weechat.network.gnutls_ca_system` or `weechat.network.gnutls_ca_user`, the TLS verification function is lost.

Consequently, any connection to a server with TLS is made without verifying the certificate, which could lead to a man-in-the-middle attack.

Connection to IRC servers with TLS is affected, as well as any connection a server made by a plugin or a script using the function `hook_connect`.

Mitigation

After changing options `weechat.network.gnutls_ca_system` or `weechat.network.gnutls_ca_user`, you must restart WeeChat.



- [Home](#)
- [Latest news](#)
- [Upcoming events](#)
- [Make a donation](#)
- [About](#)
- [Features](#)
- [Interfaces](#)
- [Screenshots](#)
- [History](#)
- [Support](#)
- [WeeChat.org](#)
- [Documentation](#)
- [Stable version](#)
- [Development version](#)
- [Old versions](#)



- [Security issues](#)
- [Download](#)
- [Stable version](#)
- [Development version](#)
- [Old versions](#)
- [Debian/Ubuntu repositories](#)
- [Scripts](#)
- [Browse scripts](#)
- [Unofficial scripts](#)
- [Python 3](#)
- [Development](#)
- [Roadmap](#)
- [Statistics](#)
- [Info](#)
- [Development blog](#) ↗

