TLS_FALLBACK_CSV

The TLS_FALLBACK_SCSV vulnerability addresses a specific issue in SSL/TLS protocols where a client and server could be forced to use a less secure version of the protocol through a downgrade attack. This security mechanism prevents such attacks by allowing the client to indicate that it is attempting a fallback connection. If the server detects this in a scenario where a higher protocol version is supported, it will reject the connection, thwarting attempts to downgrade the security of the communication.

How to fix "TLS_FALLBACK_CSV" vulnerability?

1. Enable TLS_FALLBACK_SCSV on the Server:

- On the server side, configure your SSL/TLS settings to support TLS_FALLBACK_SCSV. The method to do this depends on the server software and its SSL/TLS library.

2. **Disable Older SSL/TLS Protocols**: As part of a comprehensive approach, disable older, less secure protocols like SSL 3.0, TLS 1.0, and TLS 1.1 on your server. Focus on supporting TLS 1.2 and higher, which are more secure and less prone to certain types of downgrade attacks.

Revision #1
Created 9 November 2023 06:39:23 by Admin
Updated 9 November 2023 06:53:04 by Admin