VELO Production Issue - Bug #22300

[External Audit Findings][Android] Certificate files hardcoded inside the app

29 July 2025 10:04 AM - yap chekying

Status:	New	**Start date:**	29 July 2025
Priority:	Immediate	**Due date:**	
Assignee:	Abdul Halim Baharom	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Issue:
SSL Pinning is a security mechanism used to prevent man-in-the-middle attacks by validating the certificate of a trusted server during the SSL handshake. Developers store a list of trusted certificates within the app and use them to compare against the server certificate. Improper SSL Pinning implementation can make the app vulnerable to man-in-the-middle attacks if the certificate list is hardcoded and outdated.

Recommendation from pentester:
Developers are advised to add obfuscation to make decompilation difficult and to use public keys as variables to make reverse engineering difficult for attackers.

Please refer to attached excel for details.

History

#1 - 29 July 2025 10:06 AM - yap chekying

- Subject changed from [External Audit][Android] Certificate files hardcoded inside the app to [External Audit Findings][Android] Certificate files hardcoded inside the app

#2 - 29 July 2025 10:18 AM - Hao Ter Tai

- Assignee changed from Hao Ter Tai to Abdul Halim Baharom

Files

Copy of Audit Findings - Silver lake - ver2.xlsx	5.15 MB	29 July 2025	yap chekying