VELO Production Issue - Bug #22302

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

29 July 2025 10:07 AM - yap chekying

Status:	Assigned	**Start date:**	29 July 2025
Priority:	Immediate	**Due date:**	
Assignee:	yap chekying	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Issue:
Same as Android – developers embed a list of trusted certificates inside the app and use it to validate server certificates. If not properly implemented, this can leave the app vulnerable to man-in-the-middle attacks.

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

Please refer to attached excel for details.

History

#1 - 29 July 2025 10:22 AM - He Xi Yeo

- Status changed from New to Assigned

- Assignee changed from He Xi Yeo to yap chekying

- % Done changed from 0 to 100

The certificate is now encrypted and obfuscated before being included in app.

Files

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