AUGUST 2016

Apple iOS

Version 9.3.5

Product Description

1. The Apple iOS is Apple's mobile operating system, running on a variety of devices including the iPhone and iPad. It contains a suite of hardware dependent applications including email, phone, enterprise applications, Internet and organiser information. The Apple iOS integrates with multiple Mobile Device Management servers which provide centralised management and control of iOS devices. The Apple iOS provides advanced security features to meet confidentiality and security requirements.

Evaluation Scope

2. The scope of the ASD Cryptographic Evaluation (ACE) focused on the following functionality:
    - Protection of Data-at-Rest
    - Protection of Data-in-Transit

Protection Profile Conformance – Summary

3. Apple iOS 9.0 completed Common Criteria evaluation on 28 January 2016. This evaluation determined that the product met the assurance requirements of the Mobile Device Fundamentals Protection Profile version 2.0, and included the mandatory requirements of ASD's *Evaluation Pathway for Mobile Devices*.

ASD Findings and Recommendations

4. ASD's cryptographic evaluation applies to iOS 9.3.5, in addition to the Common Criteria evaluation. No significant cryptographic changes have been included in version 9.3.5, hence the findings of this evaluation also apply to version 9.3.5.

5. As the product has successfully completed an ACE, it can be used to downgrade the requirements of data at rest and data in transit for PROTECTED to those of UNCLASSIFIED; where the relevant protections are used and the device is configured according to the *iOS*

Hardening Configuration Guide (http://www.asd.gov.au/publications/).

6. Third-party applications are expected to use the *NSFileProtectionCompleteUnlessOpen* class when writing PROTECTED data to a device in a locked state.

7. Third-party applications are expected to use the *NSFileProtectionComplete* class when securing PROTECTED data on a device at all other times.

8. Agencies are expected to use iOS devices in Supervised mode.

9. Agencies should be aware that the reduction of storage and handling requirements for iOS 9.3.5 devices to those of UNCLASSIFIED is only in force when information is at rest. This applies only when the device is turned off or locked. Conversely, when the device is turned on and unlocked, it takes the classification of the agency network to which it is connected. Agencies should develop Standard Operating Procedures (SOPs) for the protection of classified mobile devices to mitigate the threat of lost or stolen active devices.

10. ASD has found the native Transport Layer Security (TLS) and IPsec implementations in Apple iOS 9.3.5 to be suitable for communicating PROTECTED information over public network infrastructure, when it is configured in accordance with the relevant sections of the Australian Government Information Security Manual (ISM).

ISM

11. Australian government agencies are reminded to periodically check the latest release of the ISM at www.asd.gov.au/infosec/ism/

12. Recommendations given in this Consumer Guide take precedence over those in the ISM where there is a conflict.

Further Information

13. Agencies wishing to use Apple iOS 9.3.5 devices should refer to the "Working Off-Site – Mobile Devices" section of the ISM.

14. The iOS Hardening and Configuration Guide provides controls, recommendations and information to assist agencies increase the security of their deployed solution. The guide is available at http://www.asd.gov.au/publications/.

Contact Details

15. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

16. Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.