STA-7 · Mobile Threat Catalogue

Archived: 2026-04-05 18:06:57 UTC

Mobile Threat Catalogue

Malicious Configuration Profiles

Contribute

Threat Category: Mobile Operating System

ID: STA-7

Threat Description: Malicious configuration profiles may contain unwanted CA certificates or VPN settings to route the device's network traffic through an adversary's system. The device could also potentially be enrolled into a malicious Mobile Device Management (MDM) system.[1]

Threat Origin

Malicious Profiles - The Sleeping Giant of iOS Security [2]

Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices [3]

Symantec Internet Security Threat Report 2016 [4]

Exploit Examples

Threat Advisory Semi Jailbreak [5]

YiSpecter: First iOS Malware That Attacks Non-jailbroken Apple iOS Devices by Abusing Private APIs [6]

iOS SideStepper Vulnerability Undermines MDM Services: Check Point [7]

Apple iPhone, iPad iOS 9 security flaw lets malicious apps sneak onto enterprise devices [8]

CVE Examples

Possible Countermeasures

Enterprise

To prevent attackers from creating counterfeit management profiles by signing them with stolen enterprise certificates, ensure strong security measures are used to protect both enterprise access to trusted certificate services (e.g., VeriSign) and any obtained certficates (e.g. MDM server certificates, Apple Push Notification Services certificates).

To prevent a device from accepting a malicious management profile after enrollment, use EMM/MDM solutions in combination with devices that properly verify the integrity and authenticity of device management profiles prior to their application, such as by using digitally-signed profiles.

To prevent users from accepting prompts to install malicious management profiles, educate users about the risks associated with installing an untrusted profile and ensure that enrollment processes allow users to know when management profiles are legitimate (e.g., in-person enrollment, or secure out-of-band deployment methods such as digitally-signed or encrypted e-mails.

To prevent users from installing malicious digital certificates, which can be used to greatly facilitate this form of attack, educate users about the risks associated with installing digital certifications, and ensure that installation processes allow users to know when digital certificates are legitimate (e.g., in-person enrollment, or secure out-of-band deployment methods such as digitally-signed or encrypted e-mails).

References
