28 AUG 2015 | NUMBER 73

THREAT ADVISORY
SEMI JAILBREAK

SEVERITY

4

■■■■□

THREAT TYPE

Jailbreak

IMPACT

Medium

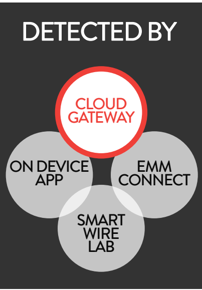
TARGET

iOS

RESPONSE

Immediate Response Required

DETECTED BY



CLOUD GATEWAY

ON DEVICE APP

EMM CONNECT

SMART WIRE LAB

SUMMARY

The Semi Jailbreak is a new form of Jailbreak, which affects iOS versions up to 8.4.1 including all iOS 8.4 compatible devices. It allows users to install applications, games and themes using the SemiJB Cydia app store, where apps may not have undergone the standard Apple vetting processes. SemiJB is not a full-blown jailbreak process, where users are granted root privileges over the device; consequently common jailbreak detection mechanisms are unable to detect it.

The process utilises a Provisioning Profile to enable the installation of the vShare App (the default SemiJB launcher), which takes up the role of SemiJB app store, where all sorts of applications are available for download including official ones and third party apps.

SECURITY IMPLICATIONS

The security implications of a Semi-Jailbroken device are not as severe as a fully jailbroken device. The key difference lies in the access to the system root. Once a device is jailbroken, the user and the app have unlimited privileges on the device and are able to interact with the system directly without a user's consent and by bypassing the iOS sandbox. SemiJB does not access the iOS root but uses a special web platform.

There are several security implications for the corporation when SemiJB devices are used by employees. Privacy can be compromised resulting in users falling victim of spying; apps built with weak security facilitate the leakage of sensitive information like usernames, passwords and location and these apps can be easily distributed through a SemiJB app store. Bad development practices and the use of custom development frameworks also increase the risk that apps contain vulnerabilities providing potential attackers with new and varied exploitation vectors. The most striking example of a privacy violating application is the vShare app itself where:

- User credentials are transferred in clear text making them visible to anyone on the wire. Considering many users commonly use the same email and password across multiple accounts, the effect of such a compromise might be devastating.
- Information about the already installed applications on the iPhone is also leaked, hence allowing any attacker to probe for other vulnerabilities and evade installed security software.
- The vShare app leaks the device name, therefore allowing the attacker to personally identify his victim; by default device names are generated from the user's real name.

The threat of SemiJB on corporate devices is particularly severe, as unverified apps from unknown developers are allowed onto the device and the corporate network. For instance, applications using Apple's private frameworks, which are blocked by iTunes, provide access to more privileged and sensitive resources than vetted applications.

REMEDIATION AND PREVENTION

Wandera's Secure Mobile Gateway actively protects its customers from a SemiJB threat by proactively detecting and blocking the vShare app from downloading onto the device. Furthermore where the vShare app is already detected as installed, Wandera will block all communication from the device to the SemiJB Cydia app store.

PREVALENCE

SemiJB has thus far been detected in 5-10 US and UK corporations across the Wandera network.