Solution Brief

Protecting Against Mobile App SSL Vulnerabilities

In these days of "there's an app for that" and the excitement that goes along with new, groundbreaking mobile app ideas, users rarely think about the ways in which mobile apps may be exposing sensitive information to man-in-the-middle (MITM) attacks—and, as a result, breaking the trust held in these supposedly secure apps. Mobile app developers also take user privacy and security lightly. Yet developers have a responsibility to protect their users' private information against the ever-growing list of cryptographic vulnerabilities such as BERserk, Heartbleed, and others.

In September 2014, CERT, the first Computer Emergency Response Team at Carnegie Mellon University, published a list of mobile apps that are vulnerable to MITM attacks because they do not properly validate SSL certificates, exposing usernames and passwords to potential attackers.[1] In January 2015—five months later—McAfee® Labs found that 18 of the top 25 most downloaded mobile apps in this list are still vulnerable due to improper digital chain validation, which is one of the most basic SSL vulnerabilities.

Because mobile app developers have not caught up to the growing demand for better privacy and security, it is important for users and enterprises to employ every available defense to maximize the safety of mobile apps.

Safeguarding against Mobile App Vulnerabilities

Here are some recommended ways to protect against exposure from vulnerable mobile apps:

- Download and install only mobile apps that are well-known, highly rated, and originate from trusted sources.
- Establish login accounts only if there are significant benefits not available to "guest" users. Create unique passwords for every account.
- Routinely test mobile apps that are used in the enterprise environment to ensure they are not exposing sensitive information due to vulnerabilities.
- Before downloading, review mobile apps privacy policies and understand what data (location, access to your social networks) the apps can access on user devices and how the data is used.

intel Security

How Intel Security Can Help Protect against Mobile App Vulnerabilities

McAfee VirusScan® Mobile

McAfee VirusScan Mobile is an antimalware system that scans and cleans mobile data, preventing corruption from viruses, Trojans, and other malicious code. McAfee VirusScan Mobile protects your mobile devices at the most critical points of exposure, including inbound and outbound emails, text messages, email attachments, and Internet downloads.

- **Detect threats in real-time:** Block malware in email, text messages, and attachments without any noticeable delay. McAfee VirusScan Mobile scans for a range of malicious threats in fewer than 200 milliseconds, providing automatic and comprehensive protection for smartphones.
- **Application privacy:** Understand what personally identifiable information your installed applications can access, to ensure that it remains secure and your data is not being needlessly exposed.
- **Reduce exposure to SSL vulnerabilities:** McAfee VirusScan Mobile provides alert notifications when applications are sending sensitive information over vulnerable connections, and classifies vulnerable applications as potentially unwanted programs (PUPs).

McAfee Complete Endpoint Protection Suites

McAfee Complete Endpoint Protection Suites integrate seamlessly with award-winning **McAfee® ePolicy Orchestrator® (McAfee ePO™)** management software. McAfee Complete Endpoint Protection Suites and McAfee ePO software enable enterprises to manage and secure mobile users from mobile malware, data exposure, and other threats.

- **Centrally managed antivirus and app reputation:** Scans applications automatically for trust reputation, while also scanning for a range of malicious threats in fewer than 200 milliseconds, providing automatic and comprehensive protection for smartphones.
- **Single pane of glass:** Secure and manage Google Android, Apple iOS, and Microsoft Windows smartphones along with traditional endpoints within McAfee ePO, leveraging its automation capabilities to deploy and enforce policies regardless of device or endpoint.
- **Policy enforcement:** Block access to corporate email if malware or PUPs are detected in apps on users' devices. Additionally leverage McAfee ePO automation to take other actions on the device (for example, wipe, move to a new area of the system tree where access to corporate VPN is denied, or other actions).

Intel Security TrueKey

TrueKey by Intel Security is an easy, safe way to log into apps on mobile phones. It removes the hassle of remembering passwords and instantly logs users into their apps, sites, and devices using multiple factors that are unique.

- **Unlock with facial math:** Log in using things that are unique to users, such as their facial math—the distance between their eyes and nose—or the devices they own.
- **Simplifies the creation and management of unique passwords:** TrueKey remembers passwords and instantly logs users into websites and apps so users don't have to remember multiple passwords.
- **Multifactor identification:** Users can boost their profiles with multiple factors that are unique to them. The more factors added, the stronger their protection becomes.

Protecting the mobile workforce from poorly implemented applications ensures your company's sensitive information is not exposed needlessly. Intel Security technology can enable your company to proactively protect itself against vulnerabilities that rattle the traditional trust model.

1. **http://www.kb.cert.org/vuls/id/582497**

61737brf_mobile-users-exposed_0215_ETMG

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com