

ECO-17 · Mobile Threat Catalogue

Archived: 2026-04-06 01:20:27 UTC

[Mobile Threat Catalogue](#)

Sign and Distribute Malicious App

[Contribute](#)

Threat Category: Mobile Application Store

ID: ECO-17

Threat Description: App developer's credentials typically have permission to push app updates to the respective app store. If these credentials are somehow obtained by an attacker, they could publish a malicious application using the developers name and reputation to aid distribution.

Threat Origin

Keep out hijackers: Secure your app store dev account [1](#)

Exploit Examples

Major security hole allows Apple passwords to be reset with only email address, date of birth (update) [2](#)

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Use app-vetting tools or services to determine that apps appear free of malicious behaviors or vulnerabilities prior to authorizing their use.

To decrease the time to detection for malicious apps, use app threat intelligence services to detect malicious apps installed on devices

Educate end users to scrutinize the permissions requested by apps, particularly if an updated version requests significantly different permissions than previous ones.

Mobile App Developer

To reduce the potential for an attacker to impersonate you to official apps stores, follow best practices to protect your developer accounts, such as using multi-factor authentication. [3](#) [4](#)

To reduce the potential for an attacker to craft malicious apps that validate against your developer account, follow best practices to protect cryptographic signing material for applications [5](#)

Mobile Device User

To decrease the time to detection for malicious apps, use Android Verify Apps feature.

References

1. G. Gruman, “Keep out hijackers: Secure your app store dev account,” InfoWorld, 5 Dec. 2014; www.infoworld.com/article/2854963/mobile-development/how-to-keep-your-app-store-dev-account-from-being-hijacked.html [↵](#)
2. C. Welch, “Major security hole allows Apple passwords to be reset with only email address, date of birth (update),” The Verge, 22 Mar. 2013; www.theverge.com/2013/3/22/4136242/major-security-hole-allows-apple-id-passwords-reset-with-email-date-of-birth [↵](#)
3. Protect your developer account, Google, 2016, <https://support.google.com/googleplay/android-developer/answer/2543765?hl=en> [accessed 8/25/16] [↵](#)
4. Security and your Apple ID, Apple, 2016, <https://support.apple.com/en-us/HT201303> [accessed 8/25/16] [↵](#)
5. Secure Your Private Key, in User Guide, <https://developer.android.com/studio/publish/app-signing.html#secure-key> [accessed 8/25/16] [↵](#)

Source: <https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-17.html>