ECO-5 · Mobile Threat Catalogue

Archived: 2026-04-05 22:46:49 UTC

Mobile Threat Catalogue

Exploit Remote Management Services

Contribute

Threat Category: Mobile OS & Vendor Infrastructure

ID: ECO-5

Threat Description: If adversaries are able to exploit cloud services that can control devices remotely, they can take advantage of this to track, locate, or wipe devices (e.g. Apple's Find My iPhone).

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

How Apple and Amazon Security Flaws Led To My Epic Hacking [1]

CVE Examples

Not Applicable

Possible Countermeasures

Mobile Device User

To prevent an attacker from gaining unauthorized access to sensitive functionality (e.g., locating or wiping a device associated with the account), enable two-factor or other strong authentication methods for user accounts on Google, Apple, or other device management and tracking services.

To detect unauthorized access to user accounts, use features from Google or others to periodically analyze account activity for suspicious logins.

Enterprise

To prevent an attacker from gaining unauthorized access to sensitive functionality (e.g., locating or wiping a device associated with the account), enable two-factor or other strong authentication methods for user accounts on Google, Apple, or other device management and tracking services.

To detect unauthorized access to user accounts, use features from Google or others to periodically analyze account activity for suspicious logins.

References

1. M. Honan, “How Apple Aan Amazon Security Flaws Led To My Epic Hacking”, Wired, 6 Aug. 2012; http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ [accessed 8/24/2016] ↩
