ECO-4 · Mobile Threat Catalogue

Archived: 2026-04-06 01:12:34 UTC

Mobile Threat Catalogue

Remote App Installation Exploit

Contribute

Threat Category: Mobile OS & Vendor Infrastructure

ID: ECO-4

Threat Description: Remote installation capabilities of app stores can be exploited to install malicious apps on mobile devices.

Threat Origin

Symantec Internet Security Threat Report 2016 [1]

Exploit Examples

How I Almost Won Pwn2Own via XSS [2]

How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication [3]

CVE Examples

Not Applicable

Possible Countermeasures

Mobile Device User

To prevent an attacker from gaining unauthorized access to remote installation functionality, enable two-factor or other strong authentication methods for user accounts on app stores.

To detect unauthorized activity, including remote installation of apps, use features from Google or others to periodically analyze account activity for suspicious logins.

Enterprise

To prevent an attacker from gaining unauthorized access to remote installation functionality, enable two-factor or other strong authentication methods for user accounts on app stores.

To detect unauthorized activity, including remote installation of apps, use features from Google or others to periodically analyze account activity for suspicious logins.

Deploy a combination of MDM, MAM, or container solutions and mobile devices that successfully enforce policies (e.g., whitelisting) that prevent unauthorized applications from being installed to managed areas of the device.

To reduce the time to detection of malicious applications, use app threat intelligence services to identify malicious apps installed on devices.

References

1. Internet Security Threat Report vol. 21, Symantec, 2016; https://docs.broadcom.com/doc/istr-16-april-volume-21-en [accessed 8/1/2022] ↩
2. J. Oberheide, “How I Almost Won Pwn2Own via XSS”, 07 Mar. 2011; https://jon.oberheide.org/blog/2011/03/07/how-i-almost-won-pwn2own-via-xss/ [accessed 8/25/2016] ↩
3. R. Konoth, V. van der Veen et al., “How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication”, in Proceedings of the 20th Conference on Financial Cryptography and Data Security, 2016; https://vvdveen.com/publications/BAndroid.pdf [accessed 8/1/2022] ↩
