APP-0 · Mobile Threat Catalogue

Archived: 2026-04-05 21:44:22 UTC

Mobile Threat Catalogue

Eavesdropping on Unencrypted App Traffic

Contribute

Threat Category: Vulnerable Applications

ID: APP-0

Threat Description: Transmission of app or device data unencrypted allows any attacker with access to the physical media channel (e.g. proximity to wireless radios) to intercept that data. Even if the data is not directly sensitive, it may in combination with other data, allow an attacker in infer sensitive information or conduct other attacks against the user or device (e.g. geo-physical tracking, social engineering, phishing, watering-hole attacks).

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Remote Code Execution as System User on Samsung Phones [1]

Insecurity Cameras and Mobile Apps: Surveillance or Exposure? [2]

Team Joch vs. Android [3]

CBS App & Mobility Website [4]

The Fork [5]

Card Crypt [6]

CVE Examples

- CVE-2015-4640
- CVE-2017-2412

Possible Countermeasures

Mobile Device User

To use HTTPS for web servers that support both HTTP and HTTPS, prepend URLs entered into the browser location bar with ‘https://’.

Mobile App Developer

Implement secure communications in apps. On iOS, use the App Transport Security feature. On Android, opt out of the use of Cleartext traffic.

Enterprise

Use app vetting tools/services that can detect the use of cleartext traffic in mobile apps before deployment within your organization.

To protect the confidentiality of enterprise data against passive interception, particularly when mobile devices may be connected to public networks (e.g. coffee shop Wi-Fi), deploy mobile VPN technologies to encapsulate potentially clear-text network traffic with a layer of strong encryption.

References

1. R. Welton, “Remote Code Execution as System User on Samsung Phones”, blog, 16 June 2015; www.nowsecure.com/blog/2015/06/16/remote-code-execution-as-system-user-on-samsung-phones/ [accessed 8/25/2016] ↩
2. J. V. Dyke, “Insecurity Cameras and Mobile Apps: Surveillance or Exposure?”, blog, 6 Jan. 2016; www.nowsecure.com/blog/2016/01/06/insecurity-cameras-and-mobile-apps-surveillance-or-exposure/ [accessed 8/25/2016] ↩
3. J. Oberheide and Z. Lanier, “Team Joch vs. Android”, presented at ShmooCon 2011, 28-30 Jan. 2011, slide 54; https://jon.oberheide.org/files/shmoo11-teamjoch.pdf [accessed 8/25/2016] ↩
4. CBS App & Mobility Website, Wandera Threat Advisory No. 192, Wandera, 23 Mar. 2016; www.wandera.com/resources/dl/TA_CBS.pdf [accessed 8/24/2016] ↩
5. The Fork, Wandera Threat Advisory No. 154, Wandera, 14 Jan. 2016; www.wandera.com/resources/dl/TA_The_Fork.pdf [accessed 8/24/2016] ↩
6. Card Crypt, Wandera Threat Advisory No. 142, Wandera, 9 Dec. 2015; www.wandera.com/resources/dl/TA_CardCrypt.pdf [accessed 8/24/2016] ↩
