APP-6 · Mobile Threat Catalogue

Archived: 2026-04-06 01:51:47 UTC

Mobile Threat Catalogue

Vulnerable Third-Party Library

Contribute

Threat Category: Vulnerable Applications

ID: APP-6

Threat Description: A mobile app may not directly contain vulnerabilities in its code, but may make calls to a third-party library that does contain vulnerabilities that are exploitable by a remote attacker.

Threat Origin

A Pattern for Remote Code Execution using Arbitrary File Writes and MultiDex Applications [1]

Unsafe Exposure Analysis of Mobile In-App Advertisements [2]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the side-loading of apps, which may bypass security checks on the app.

Deploy MAM or MDM solutions with policies that prohibit the installation of apps from 3rd party (unofficial) app stores.

Use app-vetting tools or services to identify apps that use vulnerable libraries.

References

1. R. Welton, “A Pattern for Remote Code Execution using Arbitrary File Writes and MultiDex Applications”, blog, 15 June 2015; www.nowsecure.com/blog/2015/06/15/a-pattern-for-remote-code-execution-using-

arbitrary-file-writes-and-multidex-applications/ [accessed 8/25/2016] ↩

2. M. Grace et al., “Unsafe Exposure Analysis of Mobile In-App Advertisements”, in Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks,2012, pp. 101-112; http://dl.acm.org/citation.cfm?id=2185464 [accessed 8/25/2016] ↩
