APP-8 · Mobile Threat Catalogue

Archived: 2026-04-06 00:17:04 UTC

Mobile Threat Catalogue

WebView App Vulnerable to Browser-Based Attacks

Contribute

Threat Category: Vulnerable Applications

ID: APP-8

Threat Description: A mobile app that implement a WebView, which allows it to render and potentially perform actions available in a web page, may contain vulnerabilities to common browser-based attacks, such as cross-site request forgery, cross-site scripting, and injection of malicious dynamic content (e.g., JavaScript). Further, exploits delivered over web pages may allow remote exploitation of vulnerabilities in other app components, thereby gaining access to data or functionality outside the context of the vulnerable WebView.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

WebView addJavaScriptInterface Remote Code Execution [1]

DRD13. Do not provide addJavaScriptInterface method access in a WebView which could contain untrusted content [2]

Remote code execution on Android devices [3]

CVE Examples

- CVE-2017-0587
- CVE-2017-0588
- CVE-2017-0589
- CVE-2017-0590
- CVE-2017-0591
- CVE-2017-0592

Possible Countermeasures

Enterprise

Use app-vetting tools or services to identify vulnerable applications

Use a proxy or VPN for connections to decrease the chance of success of a man-in-the-middle attack.

Mobile App Developer

Always use https URLs for WebView content.

Avoid enabling the WebView JavaScript bridge (with addJavascriptInterface) unless explicitly needed.

References

1. “WebView addJavaScriptInterface Remote Code Execution”, 24 Sept. 2013; https://labs.mwrinfosecurity.com/blog/webview-addjavascriptinterface-remote-code-execution/ [accessed 8/25/2016] ↩

2. F. Long, “DRD13. Do not provide addJavascriptInterface method access in a WebView which could contain untrusted content. (API level JELLY_BEAN or below)”, 8 Apr. 2015; www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=129859614 [accessed 8/25/2016] ↩

3. T. Sutcliffe, “Remote code execution on Android devices”, blog, 31 July 2014; https://labs.bromium.com/2014/07/31/remote-code-execution-on-android-devices/ [accessed 8/25/2016] ↩
