Stealing Videos from VLC-iOS (IDOR)

Summary

VLC for iOS was vulnerable to an unauthenticated insecure direct object reference (IDOR) which could allow a local attacker to steal media from the storage by just navigating to the source URL/IP.

This was possible by abusing a functionality in the iOS application for VLC, which allows a user to share files with others over WiFi. This can be simply done by enabling "Network **>** Sharing via WiFi" and the web-server for this functionality works on port 80(http) protocol.

Attack Vector

Let's assume a scenario where Bob & Alice are sharing a video over the WiFi using vlc-iOS, Eve could perform this attack by crawling the source IP address of Bob which would list the URL's of the videos shared between Bob & Alice.

Having said that, navigating to those URL's Eve could simply steal the video without Bob's knowledge which successfully leads to unauthenticated IDOR.

In the below image, Bob's IP is 192.168.1.135 and the hierarchy of stored videos in Bob's phone would look like,

Proof of concept

Such things can be crawled via burpsuite or you can use python scrapy to extract the URL's from the host and download the videos.

Mitigation from VLC Security team

They implemented a user-friendly authentication mechanism on VLC iOS web server for WiFi Sharing. Passcode authentication is enabled when VLC's passcode setting is enabled and the user uses the passcode that he set in VLC's settings to log into Wifi Sharing.

This was reported on 2nd Jan 2019 and patched on 10th Feb 2020 whereas fixed version was publicly released in March 2020. Post mitigation VLC published an advisory for this which you can view here[1]. Aside this issue was accepted for bounty on The Internet.

References

[1]: https://code.videolan.org/videolan/vlc-ios/blob/master/Docs/NEWS#L3
Blog URL: https://www.inputzero.io/2020/03/idor-in-vlc-ios.html
Twitter: https://twitter.com/RandomDhiraj/