INCLUDE SECURITY

Remediation Test of Open Technology Fund's client VPN Hood's Mobile application, Windows client, and Server

EXECUTIVE SUMMARY

Engagement Details

Client	Open Technology Fund's client VPN Hood
Engagement Scope	Mobile application, Windows client, and Server
Original Assessment Schedule	June 12, 2023 - July 19, 2023
Remediation Test Dates	September 07, 2023 - September 07, 2023

Remediation Test Update: Technical Findings Summary

The information below summarizes the observations of the Includesec team during the course of the remediation test intended to reproduce the findings as originally reported. The team attempted to bypass any added mitigations or protections put in place to hinder exploitation of the findings.

Finding	Risk Rating	Status
M1	Medium	Risk Accepted
I1	Informational	Risk Accepted
I2	Informational	Risk Accepted
I3	Informational	Closed (with Note)

MEDIUM-RISK FINDINGS

M1: [Android] Application Executable Signed with v1 Signature Scheme (JANUS Vulnerability)

Status: Risk Accepted

Notes:

The VPNHood team provided the following statement indicating that no remediation is planned for the finding as it is deemed to be an accepted risk:

"The APK already has APK signatures version 1 and 2 & 3. Some users have old devices with old Android versions, new Android uses newer [signatures]. Also, the program is open source and even if we remove v1, malicious person can build a new APK and add v1 [signature]. For compatibility with older devices Google recommends signing with v1. Google play store also provides APK with v1 signing mechanism to older devices."

INFORMATIONAL FINDINGS

I1: [Android] Application Data Backup Is Enabled

Status: Risk Accepted

Notes:

The **VPN Hood** team accepted the (nominal) risk for this finding with the following note:

"We intentionally enabled application data backup to allow users to back up their tokens to other devices. These tokens are used for account purposes and verification, and they do not contain any user data."

I2: [Android] Cleartext Traffic is Enabled

Status: Risk Accepted

Notes:

The **VPN Hood** team accepted the (nominal) risk of this finding with the following note:

"Considering VPNHood emulates real world and general HTTPS connections, client Apps need to use a self-signed certificate , also VpnHood directly checks the certificate via its public key hash in the access key. If you enable cleartext protection, the connection will not be established. however all connection Is https and encrypted using https certificates"

The assessment team has also adjusted the risk to **Informational** based on mitigating factors described in the finding and notes from the **VPN Hood** team.

I3: [Android] Jailbreak or Rooted Device Detection Not Implemented

Status: Closed (with Note)

Notes:

The **VPN Hood** team accepted the (nominal) risk for this finding with the following note:

"We should mention that there is no sensitive or user data stored in the application which might raise concern regarding installing on rooted devices. The application itself is open source and reverse engineering does not apply here. Besides, users need to install VpnHood on rooted devices and Android boxes and Android TVs in some cases. Also, sometimes users need to take screenshots and send them to us for support and debugging the system."