INCLUDE SECURITY

Statement of Assessment (SOA): Remediation Test of Least Authority's Gridsync application and Tahoe LAFS Android application

Include Security (IncludeSec)

IncludeSec brings together some of the best information security talent from around the world. The team is composed of security experts in every aspect of consumer and enterprise technology, from low-level hardware and operating systems to the latest cutting-edge web and mobile applications. More information about the company can be found at www.IncludeSecurity.com.

Engagement Details

IncludeSec performed a security assessment of Least Authority's Gridsync application and Tahoe LAFS Android application. The assessment team performed a 8 day effort spanning from May 17th, 2021 – May 31st, 2021, using a Standard Grey Box assessment methodology which included a detailed review of all the components described in a manner consistent with the original Statement of Work (SOW).

A remediation test of the findings as originally reported was performed on March 25th, 2022. This remediation test was intended to reproduce the original findings and bypass any added mitigations and protections put in place to hinder exploitation of the findings. At the conclusion of the remediation test, the assessment team logged the status of these finding in the table provided at the end of this SOA.

Description of Security Assessment

IncludeSec focused on the following areas of scope during the Standard Grey Box assessment of Least Authority's Gridsync Application and Tahoe LAFS Android Application:

Component	Language	Lines of Code
Tahoe (Mobile app)	Kotlin	~2,000
Gridsync Mobile Gateway Bridge (Desktop app)	Python	~10,000
Total Lines of Code	**Approximately**	**12,000**

The following tasks were conducted during the security assessment:

Information/Documentation Gathering and Configuration

At the beginning of the assessment, IncludeSec reviewed documentation and conferred with Least Authority's project manager and other designated representatives to gather background information on the areas of scope. Necessary tasks included:

- Phone calls or interviews with technical and/or business representatives to gain a solid understanding of the common workflows and user interactions.
- Configuration based on provided information, an optimal testing configuration was requested by IncludeSec to be applied to the testing environment.

Grey Box Testing

Once required information was gathered, IncludeSec performed the following activities:

Mobile Application Grey Box Testing (Tahoe)

Once required information is gathered, IncludeSec will perform the following activities:

- Mobile Application Security Testing: Using commercial tools, public tools, custom tools, and manual techniques the assessment team will identify code patterns indicative of implementation security bugs. In particular, the team seeks to determine whether attackers can identify and exploit common and advanced mobile security vulnerabilities, including:
    - Abuse of rights and permissions granted to the mobile client.
    - Side Channel Data Leakage (PII information being leaked in the form of screen snapshots, client side log files, etc.)
    - Data stored insecurely on the mobile device on the file system or as part of application footprint itself
    - Transport encryption verification (Non-SSL for sensitive pages)
    - Cipher Strength Analysis
    - Client Side Injection
    - Poor Authorization and Authentication
    - Improper Session Handling
    - Use of Untrusted Inputs to make Security Decisions
    - Reverse Engineer the application to obtain sensitive information such as cryptographic symmetric keys, passwords, etc.
    - Obtain inappropriate access to other applications or mobile device features via the client application.

Grey Box Testing of Desktop Client Application (Gridsync Mobile Gateway Bridge)

Once required information is gathered, the assessment team shall focus on the following security concerns:

- Local attack surface
    - Investigation into local privilege escalation vulnerabilities (i.e. race conditions, symlink attacks, DLL Planting, file-system permissions issues, NULL DACLs, etc.)
    - Buffer Overflows, Format String and other Memory Corruption/Trespass Attacks (as applicable)
    - Configuration issues related to the storage of sensitive information within the Windows registry, specific registry abuses
    - Cryptographic operations and storage (as applicable)

- Remote Attack surface
    - Determine whether new remotely accessible attack surface areas on the OS are opened by the client executing within the operational environment of a customer's system.
    - Attempt to attack and exploit such attack surface area.
    - Attempt to attack and exploit such attack surface area (local HTTP servers, RPC servers, UNIX sockets, etc.)

- Protocol attack surface area
  - Transport layer security usage (confidentiality and integrity of messages)
  - Privacy issues: Identify areas where user information may be accidently sent to Client's servers. (i.e. error logging, memory dumps, etc.)
  - If information collected is in an "OPT IN" manner. i.e. user is generally made aware of any information being exfiltrated by client.

A. Client Specified Concerns

Once required information is gathered, IncludeSec will address the following client-specified concerns:

- Leakage of data, especially anything that can be considered personal data, that might unintentionally give away information
- Usage of cryptography -- in particular, with regard to cipher suite selection and the generation, serialization, and storage of x509 certificates (for Gridsync)
- Correctness of the implementation, in particular, with regard to certificate-pinning (for Tahoe-LAFS mobile app)
- Inappropriate permissions and excess authority
- Denial of Service (DoS) and other security exploits that disrupt usage

Conclusion

At the conclusion of the assessment, IncludeSec categorized findings into four levels of perceived security risk: Critical, High, Medium, or Low. The risk categorizations below are guidelines that reflect best practices in the industry and may differ from Least Authority's internal perceived risk. It is common and encouraged that all clients recategorize findings based on their internal business risk tolerances. All findings are described in detail within the final report provided to Least Authority.

IncludeSec identified the following categories of findings: 0 "Critical-Risk," 0 "High-Risk," 1 "Medium-Risk," and 3 "Low-Risk."

Finding	Risk	Status
M1	Medium	Risk Accepted
L1	Low	Closed
L2	Low	Closed
L3	Low	Closed

IncludeSec advised Least Authority to prioritize and remediate as many findings found during the assessment as possible. The remediation test has shown that Least Authority has acted on recommendations as outlined in the previous chart. The assessment team recommends periodic security assessments to ensure further vulnerabilities are not introduced into future product release cycles. In the future, IncludeSec welcomes the opportunity to assist Least Authority in improving their SDLC in future engagements by providing security assessments of additional products.