Executive Summary

Synopsis
During the summer of 2022, Google engaged NCC Group to conduct a security assessment of VPN by Google One. VPN by Google One is a service that increases connection security and privacy to end users. Google provides several clients covering the most widely used operating systems; these VPN clients provide both encrypted transit and IP address dissociation for packets between user's devices and the VPN servers.

The product's security and privacy goals, as stated in the product's whitepaper, are:

- “We focus on three core principles: keeping our users' information secure, treating it responsibly, and putting our users in control.”
- “With VPN by Google One, we will never use the VPN connection to track, log, or sell your online activity.”
- “A Google-grade VPN that provides additional security and privacy to online connectivity without undue performance sacrifices.”

Scope
NCC Group's evaluation included:

- Security Design and Architecture Review
- VPN Library Code Review
- Windows Application Security Assessment
- MacOS Application Security Assessment
- Android Application Security Assessment
- iOS Application Security Assessment

Testing was performed in the production environment, having access to the relevant source code for the tested platforms.

Key Findings
The technical component analysis and source code review uncovered twenty-four initial findings in total, comprising:

- Three findings rated medium-severity.
- Ten findings rated low-severity.
- Nine findings rated as informational observations.

The most notable finding was related to the requirement of the Windows application to be executed with administrator privileges. While NCC Group did not find any software vulnerabilities in this application, potential insecure coding practices could result in a privilege escalation attack. This issue was correctly addressed by Google during the retest, and now the application is executed with user privileges.

The other two medium risk findings found were in the login process of both Windows and MacOS applications, which would allow local malicious applications to deny the availability of the service, or obtain the OAuth token sent after a successful login, by manipulating local ports temporarily opened by the applications during the login process.

Strategic Recommendations
Although no significant risks were identified in this assessment, it is recommended that the issues outlined in this report are reviewed in line with a suitably robust defense in depth approach which continuously monitors the organization's security posture.

1. https://www.gstatic.com/subscriptions/marketing_page/vpn/white_paper_4f995ab5d7c7edc3d3f14f2e0593f790.pdf
## Dashbboard

### Finding Breakdown

<table>
<thead>
<tr>
<th>Category</th>
<th>Original Assessment</th>
<th>Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical issues</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>High issues</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Medium issues</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Low issues</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Informational issues</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>

### Category Breakdown

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls</td>
<td>1</td>
</tr>
<tr>
<td>Configuration</td>
<td>6</td>
</tr>
<tr>
<td>Cryptography</td>
<td>4</td>
</tr>
<tr>
<td>Data Exposure</td>
<td>6</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>2</td>
</tr>
</tbody>
</table>

### Component Breakdown

<table>
<thead>
<tr>
<th>Component</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Application</td>
<td>3</td>
</tr>
<tr>
<td>Windows Application</td>
<td>7</td>
</tr>
<tr>
<td>iOS Application</td>
<td>2</td>
</tr>
<tr>
<td>macOS Application</td>
<td>6</td>
</tr>
<tr>
<td>vpn-libraries</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Critical**
- **High**
- **Medium**
- **Low**
- **Informational**
# Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

## Android Application

<table>
<thead>
<tr>
<th>Title</th>
<th>Status</th>
<th>ID</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Certificate Pinning</td>
<td>Reported</td>
<td>WWL</td>
<td>Low</td>
</tr>
<tr>
<td>Missing Permissions on Android Receivers</td>
<td>Reported</td>
<td>XA6</td>
<td>Info</td>
</tr>
<tr>
<td>User Email Address Stored Without Application-Level Encryption</td>
<td>Reported</td>
<td>3JC</td>
<td>Info</td>
</tr>
</tbody>
</table>

## Windows Application

<table>
<thead>
<tr>
<th>Title</th>
<th>Status</th>
<th>ID</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weaknesses in Authentication Process</td>
<td>Reported</td>
<td>LXX</td>
<td>Medium</td>
</tr>
<tr>
<td>Lack of Privilege Separation</td>
<td>Fixed</td>
<td>9W7</td>
<td>Medium</td>
</tr>
<tr>
<td>Lack of Anti-Exploit Protections</td>
<td>Reported</td>
<td>MDL</td>
<td>Low</td>
</tr>
<tr>
<td>Sensitive Data Sent in the URL Using POST Method</td>
<td>Reported</td>
<td>MWM</td>
<td>Low</td>
</tr>
<tr>
<td>Lack of Certificate Pinning</td>
<td>Reported</td>
<td>J2Q</td>
<td>Low</td>
</tr>
<tr>
<td>Application Vulnerable to DLL Injection</td>
<td>Reported</td>
<td>DDJ</td>
<td>Info</td>
</tr>
<tr>
<td>Sensitive Information Written to Debug Logs</td>
<td>Fixed</td>
<td>BQL</td>
<td>Info</td>
</tr>
<tr>
<td>Application Binaries Not Obfuscated</td>
<td>Reported</td>
<td>GUM</td>
<td>Info</td>
</tr>
<tr>
<td>Binaries Contained Debug Information</td>
<td>Reported</td>
<td>UEX</td>
<td>Info</td>
</tr>
</tbody>
</table>

## iOS Application

<table>
<thead>
<tr>
<th>Title</th>
<th>Status</th>
<th>ID</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Disables App Transport Security</td>
<td>Reported</td>
<td>VPB</td>
<td>Low</td>
</tr>
<tr>
<td>Mobile Application Data Storage Leaks GAIA ID in Log Files</td>
<td>Fixed</td>
<td>XUH</td>
<td>Low</td>
</tr>
<tr>
<td>Mobile Application Backgrounding Leaks Sensitive Info in Screenshots</td>
<td>Reported</td>
<td>RPK</td>
<td>Info</td>
</tr>
</tbody>
</table>

## macOS Application

<table>
<thead>
<tr>
<th>Title</th>
<th>Status</th>
<th>ID</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weaknesses in Authentication Process</td>
<td>Reported</td>
<td>G96</td>
<td>Medium</td>
</tr>
<tr>
<td>Sensitive Data Sent in the URL Using POST Method</td>
<td>Reported</td>
<td>6NH</td>
<td>Low</td>
</tr>
<tr>
<td>Application Vulnerable to DYLIB Hijacking</td>
<td>Reported</td>
<td>GMU</td>
<td>Low</td>
</tr>
<tr>
<td>Lack of Certificate Pinning</td>
<td>Reported</td>
<td>KE3</td>
<td>Low</td>
</tr>
<tr>
<td>Binaries Contained Debug Information</td>
<td>Not Fixed</td>
<td>B9L</td>
<td>Info</td>
</tr>
<tr>
<td>Application Binaries Not Obfuscated</td>
<td>Partially Fixed</td>
<td>DRA</td>
<td>Info</td>
</tr>
</tbody>
</table>

## vpn-libraries

<table>
<thead>
<tr>
<th>Title</th>
<th>Status</th>
<th>ID</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of Deprecated and Internal Functions</td>
<td>Reported</td>
<td>AJK</td>
<td>Low</td>
</tr>
</tbody>
</table>
4 Architecture Review Analysis

During the first two weeks of the engagement, NCC Group performed an assessment of the Google PPN VPN service to ensure its design would be able to facilitate the product’s security and privacy goals. This phase of the engagement was performed independently of any specific implementation of the design, focusing specifically on the technical concepts described in the client provided documentation listed in Client Provided Documentation, and in person interviews. Additionally, NCC Group created architecture diagrams, which details the components, trust boundaries and communication paths.

Architecture/Platform Description

The VPN by Google One is a product that endeavors to protect users in a way that reduces opportunities for manipulation, interception or analysis of network traffic by third parties in privileged positions.

The product whitepaper released by Google illustrates the contrast between a typical network connection and one protected by a VPN with the diagram shown in figure 1 below.

![Diagram of typical network connection and using the VPN from the Google whitepaper](image)

*Figure 1: Typical network connection and using the VPN from the Google whitepaper*

Scope and Architecture Diagrams

NCC Group performed an architecture assessment of both the current PPN environment as well as a future architecture that Google is expecting to begin to deploy in Q3 of 2022. During this assessment, NCC Group created three architecture diagrams. The first two diagrams document the current environment, with the first including the client portions and the second focused on the server-side architecture. The third diagram documents the future release.
Each component is described below.

**Client Components**
- **G1 APP**: The application responsible for hosting the VPN service and initializing the PPN library. It also provides notifications and account management.
- **PPN Service**: Java subclass of Android VPN service that runs in the same memory space as the host app. Responsible for the actual implementation of the Android VPN APIs.
- **Xenon**: The PPN network-switching layer. This library talks directly to Android and is responsible for switching Krypton’s data plane between Wi-Fi and cell networks.
- **Krypton Service and library**: PPN C++ library that implements data plane of the VPN, talking directly to Datapath session manager Copper.
- **Datapath Client**: Open-Source software application and communication protocol that implements VPN techniques to create secure point-to-point connections in routed or bridged configurations.

**Server Components**

- **Brass Backend**: Dataplane manager and key management service. It provides the public key of the data node. According to the request made from client device, it determines the specific dataplane node to use, programs the node with the client device's public key and receives a new public key the dataplane generates for return to the client device.

- **Copper (Session Manager)**: The exit node responsible for sending and receiving the packets from the device and the internet.

- **Zinc Backend**: The current authentication server that is responsible for authentication and authorization of the PPN service where it proxies GAIA authentications to Bronze.

- **Keyring Bucket**: Responsible for serving the public key, signing and verification requests.

- **Bridge-Proxy Backend**: talks to Bridge server to get valid Bridge token and sends to the bridge controller.

- **Bridge-Server**: Provides a valid token to the bridge-proxy.

- **Bridge Controller**: Handles requests to program the packet Processor.

- **Phosphor**: New closed source authentication server that will replace Zinc and Bronze in a future release. It provides access to the public key, authentication, signing and eligibility remote procedure calls (RPCs).

- **Bronze**: Closed source authentication server that is responsible for GAIA and G1 service authorizations which Zinc talks to and validates from.

- **Attestation Service**: A service running within the Phosphor instance that handles device attestation from Android and iOS devices.

- **DB Spanner**: Used to store the nonces that will be signed by the Attestation Service.

- **G1 Benefits**: Tells if the user has a PPN subscription.

- **Play**: Responsible for device attestation (Android).

- **GAIA**: Responsible for service authorization.

- **Packet Processor**: Provides a platform for low-level network packet processing applications.
Components

- **Brass**: Dataplane manager and key management service. It provides the public key of the data node. According to the request made from client device, it determines the specific dataplane node to use, programs the node with the client device's public key and receives a new public key that the dataplane generates to return to the client device.

- **Copper (Session Manager)**: The exit node responsible for sending/receiving the packets from the device and the internet. Selects the node of the Session Manager service based on user preference, service policy and load balancing.

- **Zinc**: Authentication server responsible for authentication and authorization of the PPN service where it proxies GAIA auth to Bronze. It is also responsible for converting an OAuth token and blinded session token into a signed blinded session token.

- **Bridge-Proxy Backend**: Talks to Bridge server to get valid Bridge token and sends it to the bridge controller.

- **Bridge-Server**: Provides a valid token to the bridge-proxy.

- **Bridge Controller**: Handles requests to program the packet Processor.

- **Bronze**: Closed source authentication server that is responsible for GAIA and G1 service authorizations which the Zinc talks to and validates from.

- **G1 Benefits**: Tells if the user has a PPN subscription.

- **GAIA**: Responsible for service authorization.

- **Cloud Spanner DB**: Stores session tokens to protect Brass from token replay attacks.

- **Key Rotator**: Generates and rotates blind-signing keys periodically using a cron job.
Components
The migration introduces Phosphor which replaces Zinc and Bronze; simplifying the client connection calling a public JSON API into Borg. The other components remain the same as described above.

- **Phosphor**: New closed source authentication server that will replace Zinc and Bronze in a future release. It provides access to the public key, authentication, signing and eligibility remote procedure calls (RPCs).
- **Attestation Service**: A service running within Phosphor instance that handles device attestation from Android and iOS devices. This service will prevent authentication from clients that have been modified.

General Conclusions
At the end of the review, NCC Group concluded that the PPN design allows Google to implement user authentication and authorization for the service in a way that isolates the user's Google identity (referred to internally as Gaia ID) from the VPN session network flows. The use of cryptographic blind signing during authorization is the traffic anonymization strategy, protecting user's identity from direct association with the VPN session token. However, as the privacy threat model considers Google itself as an adversary in a privileged position, this review also identified several techniques that could be employed to compromise user anonymity should Google choose or be compelled to actively violate its privacy claims.

It should be noted that none of these techniques were observed to be part of the product's strategy or implementation. Furthermore, the migration planned with the induction of Phosphor server include a specific component known as Attestation Service with the specific purpose of refusing authentication if the client application has been manipulated.

Privacy Claim Violation Opportunities
The subsections below enumerate the techniques that could be employed to associate the VPN traffic with subscriber's identity.
Manipulation of the client application
In the future, Google could update the client application to facilitate attribution of traffic to users. This type of compromise could occur at multiple levels within the application, such as modification of authentication and authorization flow or reporting the IPSec connection parameters.

Google implemented a new component called Attestation Service which will be added to the architecture in the upcoming migration planned to begin in Q3 2022. Attestation Service is designed to reject requests coming from manipulated client applications. Although this component is a step in the right direction, in order to prevent undesirable modifications by third parties, it can be assumed that since internal Google employees are responsible for these updates to the application; the protection given by Attestation Service can be bypassed as well. As Google operates the distribution platform (Play Store) and Attestation Service/Phosphor backend servers, an update of the client application might be performed to facilitate attribution of traffic to users.

Manipulation of cryptographic parameters
During the initial authorization phase, where the client application sends the blinded VPN authentication token along with the identity-attributable OAuth token, Google may be able to mark the blinded token in a way it can later identify by using a unique public key for the signing operation.

Instrumentation of client device traffic
After an IPSec connection is established, Google could reassociate a tunnel with a Google identity via generating specific, identifiable network traffic. An example of such a situation is outlined below, similar techniques are likely possible:

1. A Google application or website requests a resource via a tailored, unique domain name
2. The target device requests the IP address of the associated server over DNS
3. This DNS request is sent over the IPSec tunnel, and decrypted on the Copper server
4. The Copper server analyzes the unique domain name request and reports it to Google identity backends

Analysis of network metadata and metrics
Google could correlate networking information such as device source IP address and connection times to establish an association between an identity and tunneled VPN traffic. The source IP address of the initial authentication request containing the identity-attributable OAuth token will be the same as the one on tunnel traffic inbound to the Copper server. As the initial authentication request and tunnel establishment happen within a very short time frame, this represents a fairly strong associative metric. IPv6 traffic would add further confidence to the association, as IPv6 addresses are more likely to be unique and not shared by multiple devices via NAT.
Lack of Certificate Pinning

**Overall Risk**
Low

**Impact**
Medium

**Exploitability**
Low

**Finding ID**
NCC-GOLE021-WWL

**Component**
Android Application

**Category**
Cryptography

**Status**
Reported

**Impact**
TLS traffic between the application and the server can be intercepted if a trusted certificate authority is compromised; or if an attacker is able to install a malicious certificate on the user’s device and has a privileged network position.

**Description**
The authentication communications with the PPN service did not implement certificate pinning. This is a security feature which involves hard-coding the expected TLS certificate of the server (or a particular certificate authority) into the application, rather than relying on the certificate chain validation function offered by the underlying platform and the PKI infrastructure. This mitigates the risk from various active attacks which could be performed against the application’s TLS connection, and lead to attackers being able to intercept the application’s communications.

In particular, the use of certificate pinning mitigates the risk associated with one of the device’s trusted certificate authorities becoming compromised. Although this has happened on several occasions in recent years\(^2\)\(^3\), certification authorities are required to follow strict security standards, so these kind of attacks are usually performed by state sponsored or highly profile threat actors.

**Recommendation**
In order to further secure communications and information handled by the application, it is recommended to implement certificate pinning to mitigate the risk of interception when a certification authority is compromised.

Since Android 7.0 (SDK 24), applications can use the Network Security Config\(^4\) to define a list of trusted certificate hashes without manual checking being necessary. Information about this mechanism is available on Android’s developer documentation\(^5\).

For applications which need to support older devices, consider using a library with built-in support for pinning. For example, Square’s OkHttp library enables pinning with a few lines of code\(^6\).

Consider also pinning intermediate or root certification authorities instead of individual host certificates, since it reduces the risk associated with certificate handling but still provides a strong protection, as the attack surface is reduced to the specific CA pinned, and not the whole PKI infrastructure.

---


\(^4\) Android Developers - Network Security Configuration: https://developer.android.com/training/articles/security-config


In addition, it is considered a good practice to pin more than one certificate, especially when pinning individual host certificates, to reduce the risk of issues associated to a specific certificate, such as an expired certificate.

**Reproduction Steps**
1. Install a custom system CA in the mobile device (for devices with SDK >= 24), or user CA (for devices with SDK < 24)
2. Intercept the application’s SSL traffic to pass through an interception proxy
3. Verify that TLS traffic can be decrypted

**Location**
Google One for Android, version 1.157.459421718
**Missing Permissions on Android Receivers**

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Informational</th>
<th>Finding ID</th>
<th>NCC-GOLE021-XA6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Low</td>
<td>Component</td>
<td>Android Application</td>
</tr>
<tr>
<td>Exploitability</td>
<td>None</td>
<td>Category</td>
<td>Access Controls</td>
</tr>
<tr>
<td>Status</td>
<td>Reported</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Impact

Other android applications installed on the device can interact with the exported services. However, it is not exploitable due to checks inherited from the tiktok libraries.

### Description

The PPN package of the G1 Android Application exported two broadcast receivers that were not protected by Android permissions. In normal conditions, this would allow other applications installed on the Android device to interact with these receivers, causing unwanted behavior. However, the receivers expected protected intents that can only be sent by system services, and inherited methods from the tiktok libraries that ensured that the action of the intent matched the ones in the filter, avoiding the exploitation of this issue.

The following two (2) broadcast receivers were exported in the Android manifest file:

```xml
<receiver
    android:exported="true"
    android:name=".PackageReplacedPpnStateCheckReceiver_Receiver">
    <intent-filter>
        <action android:name="android.intent.action.MY_PACKAGE_REPLACED"/>
    </intent-filter>
</receiver>

<receiver
    android:exported="true"
    android:name=".BootCompletedPpnStateCheckReceiver_Receiver">
    <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
    </intent-filter>
</receiver>
```

The intent filters declared define that the expected actions are **MY_PACKAGE_REPLACED** or **BOOT_COMPLETED**. Both intents are protected and can only be broadcasted by Android system components, and therefore other applications can't send these.

The source code of the components called `startPpnIfUserEnabled`, which received the action sent as an argument. However, this function only checked that the action was one of the expected ones to log an event and would continue the execution even with other actions.

```java
if (!Strings.isNullOrEmpty(intentAction)) {
    switch (intentAction) {
    case "android.intent.action.MY_PACKAGE_REPLACED":
        clearcutLogger.logEvent(GoogleOneClientEventType.PPN_START_ON_PACKAGE_REPLACED);
        break;
    case "android.intent.action.BOOT_COMPLETED":
        clearcutLogger.logEvent(GoogleOneClientEventType.PPN_START_ON_BOOT_COMPLETED);
        break;
    }
```
This code would have allowed other applications installed in the device to directly interact with these receivers by sending explicit intents and other arbitrary actions. However, it was found that the receivers used the `IntentFilterAcledReceiver` class of the tiktok library, that checked if the intent action was expected by the intent filters, raising an exception when the action did not match with the intent filter.

**Recommendation**
As the tiktok `IntentFilterAcledReceiver` class is protecting the receivers from receiving unwanted intent actions, no action is needed. However, consideration should be given to implement android permissions for these components.

**Location**
Android application Manifest
User Email Address Stored Without Application-Level Encryption

Overall Risk Informational  Finding ID NCC-GOLE021-3JC
Impact Low  Component Android Application
Exploitability Low  Category Data Exposure
Status Reported

Impact
Unencrypted data is at risk of being exposed in rooted devices.

Description
The application did not use any application-level encryption mechanism to store the user email address on shared preferences files in the application data folder.

In non-rooted devices, as the android backup was not enabled, other applications could not access the application data folder due to file system permissions. However, the application could be run on rooted devices and other applications could ask for permission to run code as root. With this permission, the contents of any file on the device could be read.

Recommendation
Consider encrypting files and SharedPreferences using the Jetpack Security library\(^7\) where possible. The Jetpack Security library is provided by the Android team to enable secure, standardized encryption mechanisms based on the Android Keystore system\(^8\), and to ease the transition for developers.

Reproduction Steps
After enabling the VPN on the device, execute the following command on a device’s root shell:

```
cat /data/data/com.google.android.apps.subscriptions.red/shared_prefs/com.google.android.libraries.privacy.ppn.Settings.xml
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="AccountName">userEmail@gmail.com</string>
</map>
```

Location
- com.google.android.libraries.privacy.ppn.internal.PpnSettings

---

### Weaknesses in Authentication Process

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Medium</th>
<th>Finding ID</th>
<th>NCC-GOLE021-LXX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Medium</td>
<td>Component</td>
<td>Windows Application</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Low</td>
<td>Category</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>Status</td>
<td>Reported</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Impact**

A local attacker could cause a Denial of Service condition by preventing users from successfully authenticating to the VPN service and may be able to compromise the OAuth token.

**Description**

NCC Group identified that by sending a crafted HTTP request to the open local port used for authentication, the application closes the port. Once this port is closed, an attacker can open this TCP port and masquerade as this process. This can allow a local attacker to obtain the OAuth token of the user attempting to authenticate to the VPN. Additionally, once the port is closed, a VPN user can no longer authenticate to the VPN service.

If the VPN’s user authenticates by clicking the “Get Started” button, a new port is opened as the following image shows:

![Authentication open port](image)

*Figure 5: Authentication open port*

Once the user is authenticated through the web browser, this connects to the localhost port to send the auth token:

![Authentication successfully](image)

*Figure 6: Authentication successfully*
By looking into the application's implementation, it was identified that if the port is reached with an authentication GET request without parameters (e.g. http://localhost:60374/auth), the application closes the listening port. Therefore, a malicious application with no administrator privileges could monitor the open ports, send a request to close them (causing a denial of service by not allowing the authentication to succeed) and open the same port again to capture the OAuth token.

**Recommendation**

Ensure that the authentication code can properly handle unexpected user data. Alternatively, implement the authentication directly in the Google One VPN application, which would avoid the use of external applications (such as the web browser) and the need of opening a local port to receive the OAuth token.

**Location**
- g1_windows/app/auth/lib/auth.dart
Lack of Privilege Separation

**Overall Risk**  Medium  
**Impact**  Medium  
**Exploitability**  Medium  
**Finding ID**  NCC-GOLE021-9W7  
**Component**  Windows Application  
**Category**  Access Controls  
**Status**  Fixed

**Impact**
An attacker that manages to compromise the Google One VPN application's runtime process would gain administrative privileges within its host environment.

**Description**
The Google One VPN application process is required to be run with administration privileges. In systems based on Microsoft Windows, the user administrator has full access to the whole system without any restriction.

It is acknowledged that elevated privileges could be required by the Google One VPN software to manage or filter network packets, raw sockets or operating system functionalities. However, other elements such as configurations, logs, authentication communications or even parsers that introduce a large attack surface, can and should be run with limited privileges and within a sandbox (isolated environment). Under this model, even if an attacker were to find a vulnerability that could be exploited (for example in the authentication process), they would still need to identify a way to escape from the sandbox and escalate their privileges in order to obtain full control over the system.

As shown below, the `googleone.exe` process was running with high integrity level:

![Figure 7: Google One VPN application executed with high integrity level](image)

**Recommendation**
A new design based on separation of privileges could be implemented in order to reduce the risk outlined above, although due to the nature of the Google One VPN subsystem and its current state, designing and implementing this may require a significant amount of time.

In principle, the new design should ensure that actions that require high privileges are handled separately from those that have lesser requirements (such as parsers, authentication requests or protocol communications).
Lack of Anti-Exploit Protections

Overall Risk: Low
Impact: Low
Exploitability: Low
Finding ID: NCC-GOLE021-MDL
Component: Windows Application
Category: Configuration
Status: Reported

Impact
The application may be exposed to memory corruption attacks.

Description
Some of the DLL libraries and binaries that are part of the Google One VPN product did not make use of all anti-exploit protections that are available in modern Windows environments. Specifically a platform security feature called ControlFlowGuard\(^9\), which places restrictions on where and how an application can execute code. The omission of this protection can make the application and related binaries more vulnerable to exploitation.

The following is the list of configured binary protections for each of the binaries:

Main Path: “C:\Program Files\Google\VPN By Google One\1.0.2000.8"

<table>
<thead>
<tr>
<th>FileName</th>
<th>ASLR</th>
<th>DEP</th>
<th>ControlFlowGuard</th>
<th>HighentropyVA</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashpad_handler.exe</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>flutter_windows.dll</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>googleone.exe</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>wintun.dll</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

File Name: “C:\Program Files\Google\VPN By Google One\1.0.2000.9\VpnByGoogleOneService.exe"

ASLR: True
DEP: True
ControlFlowGuard: False
HighentropyVA: True

**Recommendation**

It is suggested that the Control Flow Guard mechanism is enabled when compiling the main application binary. CFG is a security feature that was created to combat memory corruption vulnerabilities, by placing restrictions on where an application can execute code. CFG extends previous exploit mitigation technologies such as /GS, DEP and ASLR.

**Location**

- crashpad_handler.exe
- flutter_windows.dll
- googleone.exe
- wintun.dll
- VpnByGoogleOneService.exe
Sensitive Data Sent in the URL Using POST Method

Overall Risk | Low
Impact       | Low
Exploitability | Low

Finding ID | NCC-GOLE021-MWM
Component  | Windows Application
Category   | Data Exposure
Status     | Reported

Impact
An attacker could intercept the communications between the thick application and the server, allowing them the ability to retrieve valid OAuth access tokens.

Description
The desktop client application sent requests to the authentication services located in oauth2.googleapis.com containing sensitive information in the URL. This exposed parameters such as client_id, client_secret and refresh_token to be stored in proxies.

```
POST /token
client_id=874847826917-0rfhjap59nhp8fpun56mm51shkfj2f.apps.googleusercontent.com&
client_secret=2ndJjPpvzenW2pGSRy-KYddM&grant_type=refresh_token&refresh_token=1%2F%2F032SarWRZ702eCgYIA
RAAGAMSWnF-L9Irklhy11RgUARdbJD02xbgHK3R8gVLrvD1kz988ycrbSMF6bdnN2FE0fwHud6KEs-fwPA
HTTP/1.1
Connection: close
Content-Type: application/json; charset=utf-8
Accept: application/json
User-Agent: PPN HttpFetcher
Content-Length: 0
Host: oauth2.googleapis.com
```

The response also contained the current access token, making it possible to retrieve this information by reusing the same request while the refresh token is valid:

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Pragma: no-cache
Date: Wed, 31 Aug 2022 13:00:58 GMT
Content-Type: application/json; charset=utf-8
Vary: X-Origin
Vary: Referer
Server: scaffolding on HTTPServer2
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29="/443"; ma=2592000,h3-065="/443"; ma=2592000,h3-046="/443"; ma=2592000,h3-043="/443"; ma=2592000,h3-042="/443"; ma=2592000,qulc="/443"; ma=2592000; v="46,43"
Accept-Ranges: none
Vary: Origin,Accept-Encoding
Connection: close
Content-Length: 487
[
```
This information should have been sent using the HTTP POST body. Note that the use of HTTPS is not an effective mitigation of this risk.

This issue has been rated to a low severity because a blinded_token is needed in order to perform the next request to the Zinc API.

**Recommendation**

While the application currently uses a POST request to send data, sensitive information (such as the client_secret and refresh_token parameters) should only be sent within the message body of the POST requests and not within the URL. Likewise, on the server-side, ensure that sensitive data is only accepted within the message body and never from the URL.

**Reproduction Steps**

1. Download and install Burp Suite/MitMProxy
2. Set the proxy up on 127.0.0.1:8080
3. Install the Burp/MitMProxy CA as Trusted Root Certification Authority on the local Windows machine.
4. Use a third-party application such as ProxyCap to force network traffic through the proxy.
5. Run the G1 application and select “Use VPN”.
6. Intercept HTTPS traffic using the proxy.
7. Check that the POST request sent the parameters client_secret and refresh_token in the URL to oauth2.googleapis.com API.

**Location**

- **Krypton library**: DesktopOAuth::RefreshAccessToken()
  [krypton\desktop\desktop_oauth.cc - line 159]
Lack of Certificate Pinning

**Overall Risk**  Low  
**Impact**  Medium  
**Exploitability**  Low  

**Finding ID**  NCC-GOLE021-J2Q  
**Component**  Windows Application  
**Category**  Cryptography  
**Status**  Reported  

**Impact**
TLS traffic between the application and the server can be intercepted if a trusted certificate authority is compromised; or if an attacker is able to install a malicious certificate on the user's laptop and has a privileged network position.

**Description**
The authentication communications with the PPN service did not implement certificate pinning. This is a security feature which involves hard-coding the expected TLS certificate of the server (or a particular certificate authority) into the application, rather than relying on the certificate chain validation function offered by the underlying platform and the PKI infrastructure. This mitigates the risk from various active attacks which could be performed against the application's TLS connection, and lead to attackers being able to intercept the application's communications.

In particular, the use of certificate pinning mitigates the risk associated with one of the device's trusted certificate authorities becoming compromised. Although this has happened on several occasions in recent years\(^\text{10}\),\(^\text{11}\), certification authorities are required to follow strict security standards, so these kind of attacks are usually performed by state sponsored or highly profile threat actors.

**Recommendation**
In order to further secure communications and information handled by the application, it is recommended to implement certificate pinning to mitigate the risk of interception when a certification authority is compromised.

Consider also pinning intermediate or root certification authorities instead of individual host certificates, since it reduces the risk associated with certificate handling but still provides strong protection, as the attack surface is reduced to the specific CA pinned, and not the whole PKI infrastructure.

---

In addition, it is considered a good practice to pin more than one certificate, especially when pinning individual host certificates, to reduce the risk of issues associated to a specific certificate, such as an expired certificate.

**Reproduction Steps**
1. Install the Burp Proxy CA in the Keychain.
2. Intercept the application's SSL traffic to pass through an interception proxy such as Burp Proxy.
3. Verify that TLS traffic can be decrypted.
Application Vulnerable to DLL Injection

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Informational</th>
<th>Finding ID</th>
<th>NCC-GOLE021-DDJ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Low</td>
<td>Component</td>
<td>Windows Application</td>
</tr>
<tr>
<td>Exploitability</td>
<td>None</td>
<td>Category</td>
<td>Configuration</td>
</tr>
<tr>
<td>Status</td>
<td>Reported</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Impact**
Under specific circumstances the application could load and process malicious DLL files.

**Description**
The main executable named `googleone.exe` was traced and analysed as part of the assessment, and was found potentially vulnerable to DLL injection as DLLs were loaded in a default, insecure manner.

When DLLs are loaded without a fully-qualified path name being specified, Windows will search through a known set of directories. Should an attacker place a file with the same name as the DLL in one of these directories, and the system finds it before the correct version, it will be loaded; providing a vector for possible privilege escalation or other attacks.

It should be noted that when an application needs to load a DLL it will go through the following order:

- The directory from which the application is loaded
- `C:\Windows\System32`
- `C:\Windows\System`
- `C:\Windows`
- The current working directory
- Directories in the system PATH environment variable
- Directories in the user PATH environment variable

The following picture from `Process Monitor` software shows the analysis of the application where a number of DLLs being loaded without success by the application when executed:
Figure 9: DLLs loaded upon execution of the main executable

It can be observed that the installer was looking for a number of DLLs placed in the location where the installer is run with NAME NOT FOUND results, which means that if an attacker is able to place a malicious file named as IPHLPAPI.DLL (as highlighted in the above evidence) within the same folder (such as C:\Program Files\Google\VPN By Google One\1.0.2000.8 in this case) an attacker could perform malicious activities; such as remotely obtain control over the user's computer.12 13 14 15

All DLL files were obtained from C:\Windows\System32, as none of them were missing (which may cause the file to be obtained from non-privileged folders) it would require administrator privileges to perform this attack and therefore this finding was rated as informational.

**Recommendation**

Several methods exist for ensuring that only the correct DLL is loaded. When using `LoadLibrary`, `LoadLibraryEx`, `CreateProcess`, or `ShellExecute`, specify fully-qualified paths:

- Use the `LOAD_LIBRARY_SEARCH` flag with `LoadLibraryEx`.

• Use the LOAD_LIBRARY_SEARCH flag SetDefaultDllDirectories. This will allow you to establish the order in which the process will search for DLLs. AddDllDirectory or SetDllDirectory can be used to alter this list.
• Use DLL redirection. This involves creating an empty file called «appname».local, which should be placed in the application directory, as should the DLLs to be used.
Sensitive Information Written to Debug Logs

Overall Risk | Informational
Impact | Undetermined
Exploitability | None

Finding ID | NCC-GOLE021-BQL
Component | Windows Application
Category | Data Exposure
Status | Fixed

Impact
An attacker who obtains access to the application's log files would be able to view service access information such as authentication and authorization tokens, and sensitive parameters such as client_secret, client_id, and PKCE codes.

This information could be used to authorize another application to use the VPN service while the OAuth token remains valid.

Description
Authentication (OAuth) and authorization (blinded) tokens, as well as other sensitive information were written to debug log files. A suitably-placed attacker or malicious user would have access to those files, gaining access to the service for an undetermined amount of time.

An example of sensitive data being written to log files can be seen below, where the OAuth-related requests are registered:

```
I0902 07:52:52.687399    9868 http_fetcher.cc:143] WinHttpRequestHeaders successful
  "gM6gBYrXF4wZPh0owyfbGLY+qEOaxHK/USkQPWEiC+1hQIFPL8g",

  "oauth_token": "ya29.a0AVA9y1tTVcH_lsjZo4kRB79M6nrsZvF2sYFqFna19SKYn1E8g1b8MzRHkPwqMzQB7zYhmbs2zsd2dXXG"
  "public_key_hash": "xy0GxTH9BnDrPD/OEIG3+UERjPFB1le4d5RRdX5b8w="
  "service_type": "g1"
)
```

There are other instances where client information is also stored in debug logs:

```
```

28 / 52 – Finding Details – Windows Application
The severity for this issue was set to informational because this was only observed in debug logs.

**Recommendation**
Review the discovered instances and ensure that sensitive information is suitably stripped before being committed to log files.

Investigate whether static analysis could be utilized to identify new instances of this class of issue during development.

**Reproduction Steps**
1. Install and run the Google One application normally (including the VPN service).
2. Navigate to the debug log folder:
   - (C:\Users\<USER>\AppData\Local\Google\GoogleOne\debug\).
3. Search sensitive information, such as “oAuth” or “token” in all files.

**Location**
C:\Users\<USER>\AppData\Local\Google\GoogleOne\debug\ppn_debug_20220902_075251.9400897.txt
**Application Binaries Not Obfuscated**

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Informational</th>
<th>Finding ID</th>
<th>NCC-GOLE021-GUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Undetermined</td>
<td>Component</td>
<td>Windows Application</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Undetermined</td>
<td>Category</td>
<td>Configuration</td>
</tr>
<tr>
<td>Status</td>
<td>Reported</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Impact**
The lack of code obfuscation means that it is relatively easy to determine the structure and functionality of the application, and to analyse the binary for suitable locations to modify the application behavior.

**Description**
Application binaries and libraries were not obfuscated by using an executable binary obfuscator, as shown in the image below.

![Figure 10: Application binaries are not obfuscated](image)

**Recommendation**
Consider using a binary or source-level obfuscation system to obfuscate the application. Additionally, commercially available binary obfuscation systems may also provide runtime protection of memory contents.

However, it is worth noting that all binary obfuscation can be defeated, and only serves to deter casual attackers and slow down skilled and motivated attackers. Additionally, due to the way binary executable obfuscation works, using it may remove platform-level mitigations and thus weaken the authentication system's security posture in other ways. It is worth noting that code signing will typically be mutually exclusive with binary obfuscation, requiring a business decision to be made as to whether to make the authentication system more difficult to reverse engineer or more difficult to modify.
Binaries Contained Debug Information

**Overall Risk**  Informational
**Impact**  Undetermined
**Exploitability**  Undetermined

**Finding ID**  NCC-GOLE021-UEX
**Component**  Windows Application
**Category**  Data Exposure
**Status**  Reported

**Impact**
While not a direct security issue, the presence of this information in the binaries makes reverse engineering efforts much simpler. Reverse engineering all or part of a binary is often a key step in producing a reliable exploit.

**Description**
Application binaries and DLLs contained debug information. Evidence of the issue can be seen in the screenshot below:

![Figure 11: Binaries contained debug information](image)

**Recommendation**
Software build rules should be modified to remove debug symbols in production releases. Debug strings should be out of the production code. If this is a concern for diagnosing field returns, then consider replacing them with macros that revert to simple file and line number prints (for example using `FILE` and `LINE` macros). Post-processing of the now obfuscated logs can then be used to recover the original print statements for debugging purposes. Failure messages should be simplified so as not to reveal the detailed operation of the program. Avoid using function names and consider simple error numbers.

**Location**
Windows Application
### Finding Details – iOS Application

**Application Disables App Transport Security**

**Overall Risk**  
Low

**Impact**  
Medium

**Exploitability**  
Low

**Finding ID**  
NCC-GOLE021-VPB

**Component**  
iOS Application

**Category**  
Cryptography

**Status**  
Reported

---

**Impact**

When ATS is disabled by the application, an attacker is more easily able to intercept HTTP traffic between the mobile application and back-end services.

**Description**

As of iOS version 9, a new App Transport Security (ATS) feature was added that can enhance the security afforded to data in transit. When ATS is fully enabled, a mobile application's HTTP connections must use HTTPS and meet certain minimum certificate, protocol, and cipher suite criteria. In iOS this feature is enabled by default, but was found to be explicitly disabled for the Google One application.

This is demonstrated by observing that within the application's `Info.plist` file, the `NSAllowsArbitraryLoads` flag was set to `true`, as shown below:

```xml
<key>NSAppTransportSecurity</key>
<dict>
  <key>NSAllowsArbitraryLoads</key>
  <true/>
</dict>
```

**Recommendation**

The `NSAllowsArbitraryLoads` flag should be explicitly set to `false`.16

**Reproduction Steps**

Run objection framework17:

1. `$ objection -g com.google.one explore`
2. `com.google.one on (iPhone: 14.7.1) [usb] # ios plist cat Info.plist`

**Location**

ios/Info.plist

---

17. Objection: [https://github.com/sensepost/objection][18]
Mobile Application Data Storage Leaks GAIA ID in Log Files

Overall Risk  | Low
---|---
Impact  | Low
Exploitability  | Low

Finding ID  | NCC-GOLE021-XUH
Component  | iOS Application
Category  | Data Exposure
Status  | Fixed

Impact
By knowing a user's GAIA ID, an attacker can search it in other Google services, and find out more details about the user.

Description
Potentially sensitive data such as the GAIA ID was observed being logged by the application. Please note that on modern devices, sandboxing prevents apps from reading the logs of other apps on the device, limiting the exploitability of this issue.

Historically, mobile operating systems provided relatively weak protections against attacks across different mobile applications, and attacks that assume physical access to a locked device. All recent versions of iOS now guarantee strong sandboxing and device-level encryption which, in most cases, completely eliminates the impact of those attack vectors under a typical threat model. For most applications, no additional protections are needed beyond making use of the recommended data storage functionality provided by the operating system. If an attacker gains access to a user's unlocked mobile device, they may be able to read sensitive application data that would not otherwise be accessible.

The iOS application stored the user's GAIA ID in log files in the device, as shown below:

Recommendation
On iOS, all application data can generally be stored using the built-in Data Protection classes which the OS provides for automatic file-based encryption. Critically-sensitive data such as passwords can be stored in the Keychain using Keychain Item Attributes to restrict access to the secret.
Reproduction Steps

1. $ sftp root@IP_jailbreak_device
2. $ cd /var/mobile/Containers/Data/Application/APP_ID/Caches/
   com.google.one.logsReport/
3. Download current.log file stored locally in the device

Location
/var/mobile/Containers/Data/Application/APP_ID/Caches/com.google.one.logsReport/
current.log

Mobile Application Backgrounding Leaks
Sensitive Info in Screenshots

Impact
The application did not hide screenshots shown in the list of recent applications. With physical access to an unlocked device, an attacker may be able to see information in these screenshots.

Description
When an iOS application is closed (or backgrounded), iOS takes a snapshot of the current screen content and stores it in an encrypted, sandboxed file on the device. Information on the screen at the time of closing is therefore disclosed through this screenshot and can be read by an attacker who has physical access to the unlocked device.

Some snapshots of the current screen were stored locally in the file path /Library/SplashBoard/Snapshot/sceneID/com.google.one-default/ on the device, as shown below:

![Figure 13: Mobile Application Backgrounding Leaks Info in Screenshots](image)

Recommendation
On iOS, there are three unique events that need to be handled (in iOS 10+):

1. `func applicationWillResignActive(UIApplication)` – Triggered when the app is about to become inactive (for example, on a double-tap of the home button to bring up the task switcher)
2. `func applicationDidEnterBackground(UIApplication)` – Triggered when the app enters the background state (for example, when the home button is pressed)
3. `func applicationProtectedDataWillBecomeUnavailable(UIApplication)` – Triggered when protected files become unavailable (for example, when the screen lock button is pressed)

Event handlers should be used for all three events in order to hide sensitive information from being captured in screenshots when the application makes various state transitions. More information can be found on these events in Apple’s documentation on the UIApplicationDelegate object.

**Reproduction Steps**
1. `$ sftp root@IP_jailbreak_device`
2. `$ cd /var/mobile/Containers/Data/Application/APP_ID/Library/SplashBoard/Snapshot/sceneID/com.google.one-default/`
3. Download the snapshots stored locally in the device

**Location**
/var/mobile/Containers/Data/Application/APP_ID/Library/SplashBoard/Snapshot/sceneID/com.google.one-default/

---

Finding Details – macOS Application

Weaknesses in Authentication Process

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Medium</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Low</td>
</tr>
<tr>
<td>Finding ID</td>
<td>NCC-GOLE021-G96</td>
</tr>
<tr>
<td>Component</td>
<td>macOS Application</td>
</tr>
<tr>
<td>Category</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>Status</td>
<td>Reported</td>
</tr>
</tbody>
</table>

**Impact**

A local attacker could cause a Denial of Service condition by preventing users from successfully authenticating to the VPN service and may be able to compromise the OAuth token.

**Description**

NCC Group identified that by sending a crafted HTTP request to the open local port used for authentication, the application closes the port. Once this port is closed, an attacker can open this TCP port and masquerade as this process. This can allow a local attacker to obtain the OAuth token of the user attempting to authenticate to the VPN. Additionally, once the port is closed, a VPN user can no longer authenticate to the VPN service.

The following image shows a new port being opened after a user authenticates to the VPN service.

![Figure 14: Authentication open port](image)

Once the user is authenticated through the web browser, it connects to the localhost port to send the authentication token:
By looking into the application's implementation, NCC Group identified that if the port is reached with an authentication GET request without parameters (e.g. http://localhost:58233/auth), the application closes the listening port. Therefore, a malicious application without administrator privileges could monitor the open ports, send a request to close them (causing a denial of service by not allowing the authentication to succeed) and then open the same port again to capture the OAuth token.

**Recommendation**
Ensure that the authentication code can properly handle unexpected user data. Alternatively, implement the authentication directly in the Google One VPN application, which would avoid the use of external applications (such as the web browser) and the need of opening a local port to receive the OAuth token.

**Location**
- g1_macos/app/auth/lib/auth.dart
Sensitive Data Sent in the URL Using POST Method

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Finding ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>NCC-GOLE021-6NH</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>macOS Application</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exploitability</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Data Exposure</td>
</tr>
</tbody>
</table>

| Status | |
|--------||
| Reported | |

**Impact**

An attacker could intercept the communications between the thick application and the server, allowing them the ability to retrieve valid OAuth access tokens.

**Description**

Authentication requests to the OAuth2 API oauth2.googleapis.com were submitted in the URL using the HTTP POST method. This resulted in secrets such as client_secret and refresh_token being sent as plaintext in the URL. These secrets should be sent in the body of the POST request instead of the URL.

This meant that secrets could be stored on any proxy servers between the thick application and the server.

Note that the use of HTTPS is not an effective mitigation of this risk.

This issue has been rated to a low severity because a blinded_token is needed in order to perform the next request to the Zinc API.

**Recommendation**

While the application currently uses a POST request to send data, sensitive information (such as the client_secret and refresh_token parameters) should only be sent within the message body of the POST requests and not within the URL. Likewise, on the server-side, ensure that sensitive data is only accepted within the message body and never from the URL.

**Reproduction Steps**

1. Download and install Burp Suite
2. Set the proxy up on 127.0.0.1:8080
3. Install the Burp CA as Trusted Root on the Keychain
4. Go to: macOS System Preferences -> Network -> Proxies and configured HTTP
5. HTTPS to proxy through 127.0.0.1:8080
6. Run the G1 application and “Use VPN”
7. Intercept HTTPS traffic using Burp Proxy
8. Check that the POST request sent the parameters client_secret and refresh_token in the URL to oauth2.googleapis.com API.

Request:

```
POST /token?
client_id=874847826917-0rfhjap59hlpn56mm51ssshfj2f.apps.googleusercontent.com&client_sec
```
Location
- macOS Application
Application Vulnerable to DYLIB Hijacking

Overall Risk: Low
Impact: Low
Exploitability: Low
Finding ID: NCC-GOLE021-GMU
Component: macOS Application
Category: Configuration
Status: Reported

Impact
Under specific circumstances the application could load and process malicious DYLIB files.

Description
The main executable named `VPN_by_Google_One` was traced and analyzed as part of the assessment, and was found potentially vulnerable to DYLIB injection as the DYLIB files were loaded in a default, insecure manner.

The following scenarios could be a vector for possible privilege escalation or other attacks:

- `LC_LOAD_WEAK_DYLIB` that reference a non-existent DYLIB.
- `LC_LOAD*_DYLIB` with @rpath'd import and multiple LC_RPATHs with the run-path dependent library not found in a primary run-path search path.

The following command shows all the DYLIBs being loaded by the application when executed:

```
$ otool -l /Applications/VPN_by_Google_One.app/Contents/MacOS/VPN_by_Google_One
...
Load command 20
   cmd LC_LOAD_WEAK_DYLIB
   cmdsize 112
   name /System/Library/Frameworks/SystemExtensions.framework/Versions/A/SystemExtensions (offset 24)
   time stamp 2 Thu Jan  1 01:00:02 1970
   current version 1.0.0
   compatibility version 1.0.0
...
```

A file search shows that the DYLIB was not found in the system:

```
$ ls /System/Library/Frameworks/SystemExtensions.framework/Versions/A/SystemExtensions
ls: /System/Library/Frameworks/SystemExtensions.framework/Versions/A/SystemExtensions: No such file or directory
```

If weak linking is used, such as the `LC_LOAD_WEAK_DYLIB` function, an application will still execute even if an expected DYLIB is not present. Weak linking enables developers to run an application on multiple macOS versions as new APIs are added.

The following picture from TaskExplorer software shows the analysis of the application where a number of DYLIBs being loaded without success by the application when executed:

22. Dylib-hijacking-os-x
23. MITRE Dylib Hijacking
24. TaskExplorer
Recommendation
Set directory access controls to prevent file writes to the search paths for applications, both in the folders where applications are run from and the standard DYLIB folders.²⁵

Monitor for dynamic libraries being loaded. Run path dependent libraries can include LC_LOAD_DYLIB, LC_LOAD_WEAK_DYLIB, and LC_RPATH. Other special keywords recognized by the macOS loader are @rpath, @loader_path, and @executable_path.²⁶ These loader instructions can be examined for individual binaries or frameworks using the otool -l command. Objective-See's Dylib Hijacking Scanner can be used to identify applications vulnerable to DYLIB hijacking.

Location
• VPN_by_Google_One.app

²⁵. MITRE Dylib Hijacking
²⁶. Run-Path Dependent Libraries
Lack of Certificate Pinning

Overall Risk: Low
Impact: Medium
Exploitability: Low
Finding ID: NCC-GOLE021-KE3
Component: macOS Application
Category: Cryptography
Status: Reported

Impact
TLS traffic between the application and the server can be intercepted if a trusted certificate authority is compromised; or if an attacker is able to install a malicious certificate on the user's laptop and has a privileged network position.

Description
The authentication communications with the PPN service did not implement certificate pinning. This is a security feature which involves hard-coding the expected TLS certificate of the server (or a particular certificate authority) into the application, rather than relying on the certificate chain validation function offered by the underlying platform and the PKI infrastructure. This mitigates the risk from various active attacks which could be performed against the application's TLS connection, and lead to attackers being able to intercept the application's communications.

In particular, the use of certificate pinning mitigates the risk associated with one of the device's trusted certificate authorities becoming compromised. Although this has happened on several occasions in recent years\textsuperscript{27,28}, certification authorities are required to follow strict security standards, so these kind of attacks are usually performed by state sponsored or highly profile threat actors.

Recommendation
In order to further secure communications and information handled by the application, it is recommended to implement certificate pinning to mitigate the risk of interception when a certification authority is compromised.

Consider also pinning intermediate or root certification authorities instead of individual host certificates, since it reduces the risk associated with certificate handling but still provides strong protection, as the attack surface is reduced to the specific CA pinned, and not the whole PKI infrastructure.

In addition, it is considered a good practice to pin more than one certificate, especially when pinning individual host certificates, to reduce the risk of issues associated to a specific certificate, such as an expired certificate.

Reproduction Steps
1. Install the Burp Proxy CA in the Keychain
2. Intercept the application's SSL traffic to pass through an interception proxy such as Burp Proxy
3. Verify that TLS traffic can be decrypted

\textsuperscript{27} DigiNotar - Issuance of fraudulent certificates: https://en.wikipedia.org/wiki/DigiNotar#Issuance_of_fraudulent_certificates
Location
- VPN_by_Google_One.app
Binaries Contained Debug Information

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Informational</th>
<th>Finding ID</th>
<th>NCC-GOLE021-B9L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Undetermined</td>
<td>Component</td>
<td>macOS Application</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Undetermined</td>
<td>Category</td>
<td>Data Exposure</td>
</tr>
<tr>
<td>Status</td>
<td>Not Fixed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Impact

While not a direct security issue, the presence of this information in the binaries makes reverse engineering efforts much simpler. Reverse engineering all or part of a binary is often a key step in producing a reliable exploit.

Description

Application binaries and DLLs contained debug information. Evidence of the issue can be seen in the screenshot below:

![Figure 17: Binary contained debug information](image)

Recommendation

Software build rules should be modified to remove debug symbols in production releases. Debug strings should be out of the production code. Post-processing of the now obfuscated logs can then be used to recover the original print statements for debugging purposes. Failure messages should be simplified so as not to reveal the detailed operation of the program. Avoid using function names and consider simple error numbers.

Reproduction Steps

1. Open VPN_by_Google_One binary using a Reverse Engineering framework
2. Analyse the VPN_by_Google_One binary
3. Search for strings like “.cc”
Location
  • VPN_by_Google_One.app/Contents/MacOS/VPN_by_Google_One

Retest Results
2022-10-21 – Not Fixed
No changes were seen in the new binaries tested, all the information shown in the evidence above was still present.
Application Binaries Not Obfuscated

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Informational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Undetermined</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Undetermined</td>
</tr>
</tbody>
</table>

**Finding ID**  
NCC-GOLE021-DRA

**Component**  
macOS Application

**Category**  
Configuration

**Status**  
Partially Fixed

**Impact**
The lack of code obfuscation means that it is relatively easy to determine the structure and functionality of the application, and to analyse the binary for suitable locations to modify the application behavior.

**Description**
Application binaries and libraries were not obfuscated by using an executable binary obfuscator, as shown in the image below.

![Figure 18: No obfuscation](image)

**Recommendation**
Consider using a binary or source-level obfuscation system to obfuscate the application. Additionally, commercially available binary obfuscation systems may also provide runtime protection of memory contents.

However, it is worth noting that all binary obfuscation can be defeated, and only serves to deter casual attackers and slow down skilled and motivated attackers. Additionally, due to the way binary executable obfuscation works, using it may remove platform-level mitigations and thus weaken the authentication system’s security posture in other ways. It is worth noting that code signing will typically be mutually exclusive with binary obfuscation, requiring a business decision to be made as to whether to make the authentication system more difficult to reverse engineer or more difficult to modify.
**Location**
- VPN_by_Google_One.app/Contents/MacOS/VPN_by_Google_One

**Retest Results**
**2022-10-21 – Partially Fixed**
The VPN by Google One binary shown that some of the function names were obfuscated, but a number of them were still visible:

```plaintext
+[NSFileHandle(GTMFileHandleLogWriter)_fileHandleForLoggingAtPath:mode:]  
+[NSURL(AppGroupContainer)_applicationSupportFileDirectory]  
+[NSURL(AppGroupContainer)_googleOneAppGroupContainer]  
+[NSURL(AppGroupContainer)_googleOneAppGroupName]  
+[NSURL(AppGroupContainer)_googleOneCrashpadDirectoryPath]  
+[NSURL(AppGroupContainer)_googleOneNetworkExtensionDataDirectory]  
+[NSURL(AppGroupContainer)_googleOnePPNEnabledDatesFilePath]  
+[NSURL(AppGroupContainer)_googleOnePPNLogDirectory]  
+[NSURL(AppGroupContainer)_googleOnePPNLogPath]  
+[NSURL(AppGroupContainer)_googleOnePPNMacOSLogPath]  
+[NSURL(AppGroupContainer)_googleOnePPNSessionFilePath]  
+[NSURL(AppGroupContainer)_googleOnePPNStatusDataFilePath]  
+[NSURL(AppGroupContainer)_googleOnePPNToggleStatusFilePath]  
+[NSURL(AppGroupContainer)_googleOnePPNVPNSettingsFilePath]
```
Use of Deprecated and Internal Functions

Impact
Use of internal library functions could result in security checks being modified or rendered ineffective if the library is modified over time.

Description
The `SetBlindingPublicKey` function uses Tink functions such as `ValidateRsaModulusSize`, `ValidateRsaPublicExponent` and `BoringSslRsaFromRsaPublicKey` to validate and set public key properties. While the validation is correct, these functions are intended to be internal to the Tink library and are not for external consumption. As an example, `ValidateRsaPublicExponent` contains the following comments in `subtle_util_boringssl.h`:

```c
ABSL_DEPRECATED("Use of this function is discouraged outside Tink.")
static inline crypto::tink::util::Status ValidateRsaPublicExponent(
    absl::string_view exponent) {
  return internal::ValidateRsaPublicExponent(exponent);
}
```

Using internal functions should be avoided since such functions may disappear at any time, leading to application crashes or public key validation being rendered ineffective.

Recommendation
These Tink functions should not be called directly and it is recommended to transition to publicly maintained validation or, include these checks in the VPN library code directly.

Location
/VPN Library Code/krypton/crypto/session_crypto.cc
10 Finding Field Definitions

The following sections describe the risk rating and category assigned to issues NCC Group identified.

Risk Scale
NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. The risk rating is NCC Group's recommended prioritization for addressing findings. Every organization has a different risk sensitivity, so to some extent these recommendations are more relative than absolute guidelines.

Overall Risk
Overall risk reflects NCC Group's estimation of the risk that a finding poses to the target system or systems. It takes into account the impact of the finding, the difficulty of exploitation, and any other relevant factors.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Implies an immediate, easily accessible threat of total compromise.</td>
</tr>
<tr>
<td>High</td>
<td>Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.</td>
</tr>
<tr>
<td>Medium</td>
<td>A difficult to exploit threat of large-scale breach, or easy compromise of a small portion of the application.</td>
</tr>
<tr>
<td>Low</td>
<td>Implies a relatively minor threat to the application.</td>
</tr>
<tr>
<td>Informational</td>
<td>No immediate threat to the application. May provide suggestions for application improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.</td>
</tr>
</tbody>
</table>

Impact
Impact reflects the effects that successful exploitation has upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.</td>
</tr>
<tr>
<td>Medium</td>
<td>Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.</td>
</tr>
<tr>
<td>Low</td>
<td>Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.</td>
</tr>
</tbody>
</table>

Exploitability
Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>
### Rating

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.</td>
</tr>
</tbody>
</table>

### Category

NCC Group categorizes findings based on the security area to which those findings belong. This can help organizations identify gaps in secure development, deployment, patching, etc.

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls</td>
<td>Related to authorization of users, and assessment of rights.</td>
</tr>
<tr>
<td>Auditing and Logging</td>
<td>Related to auditing of actions, or logging of problems.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Related to the identification of users.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Related to security configurations of servers, devices, or software.</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Related to mathematical protections for data.</td>
</tr>
<tr>
<td>Data Exposure</td>
<td>Related to unintended exposure of sensitive information.</td>
</tr>
<tr>
<td>Data Validation</td>
<td>Related to improper reliance on the structure or values of data.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Related to causing system failure.</td>
</tr>
<tr>
<td>Error Reporting</td>
<td>Related to the reporting of error conditions in a secure fashion.</td>
</tr>
<tr>
<td>Patching</td>
<td>Related to keeping software up to date.</td>
</tr>
<tr>
<td>Session Management</td>
<td>Related to the identification of authenticated users.</td>
</tr>
<tr>
<td>Timing</td>
<td>Related to race conditions, locking, or order of operations.</td>
</tr>
</tbody>
</table>
11 Client Provided Documentation

The following design documentation was provided to NCC Group by Google sharing documents with a Partner Google account set for this project:

- Debug logs details and monitoring procedures: Debug and Production_Monitoring
- Guide to instance deployment and rollback in production and locally: Deployment and Rollback
- Krypton and Xenon in depth architecture: Krypton and Xenon Details
- Migration plan to a new authentication infrastructure: Phosphor Migration Plan.docx
- Phosphor in depth architecture: Phosphor_PPN ServiceType mux.docx
- Design definition for the authentication in the Borg internal network: PPN Auth on Borg Detailed Design.docx
- Authentication design and integration with Google One services: PPN Authentication and G1 Integration.docx
- Key rotation procedure in depth: PPN Key Rotation - Markdown Export.docx
- Attestation Service definition and expectations: PPN Mithril.docx
- Resources for newcomers and general architecture: PPN Onboarding Resources and Architecture.docx
- Key rotation overview and glossary: PPN Signing Key Rotation, Glossary, DNS and APN Sections.docx
- Local setup for Windows and MacOS tests: PPN Windows and MacOS Setup and Marconi Process.docx
- Proposal to implement a new authentication method: Proposal_PPN Borg Authentication.docx
- Public Google PPN VPN whitepaper: white_paper_4f995ab5d7c7eda3d3f14f2e0593f790.pdf
- How is enforced the quota during PPN authentication to prevent service abuse: PPN per-user Quota.docx

The following documents were used as working documents for writing questions and answers:

- NCC Questions-27-7-2022
- NCC Questions-28-7-2022
- NCC Questions-29-7-2022
- NCC Questions-2-8-2022