Google Enterprise API Security Assessment

Google

April 7, 2022 – Version 1.2

Prepared for

Eugene Liderman

Mike Burr

Prepared by

Simon Watson

Executive Summary

Synopsis

During the autumn of 2021, Google engaged NCC Group to perform a review of the Android 12 Enterprise API to evaluate its compliance with the Security Technical Implementation Guides (STIG) matrix provided by Google.

This assessment was also performed with reference to the Common Criteria Protection Profile for Mobile Device Fundamentals (PPMDF),[1] from which the STIG was derived.

Due to the limited nature of the testing, certain elements of the STIG requirements are expected to be covered separately either via FIPS 140-2 or Common Criteria Evaluation.

Scope

NCC Group's evaluation included:

- **Validation of Individual STIG Controls**: all individual controls detailed as part of the STIG (approximately 120 controls) were, where possible, validated by NCC Group to ensure that appropriate protections were applied as expected.
- **Review of Attack Surface with STIG applied**: with the security controls applied, the remaining attack surface was reviewed against the threats identified in the PPMDF to attempt to identify any weaknesses.

These threats included:

- Network Eavesdrop - An attacker is positioned on a wireless communication channel or elsewhere on the network infrastructure.
- Network Attack - An attacker is positioned on a wireless communication channel or elsewhere on the network infrastructure.
- Physical Access - An attacker with physical access may attempt to access user data on the mobile device including credentials. (**Note**: intrusive attacks requiring dismantling of test device were not in scope)
- Malicious Application - Applications loaded onto the mobile device may include malicious or exploitable code.
- Persistent Presence - Persistent presence on a device by an attacker implies that the device has lost integrity and cannot regain it.

Testing was performed on:

- Google Pixel 4A 5G device (SN: 14241JECB068650)
- Android 12 Beta 5 (Build: SPB5.210812.002)
- Google's 'Android at Work' demonstrator platform

Limitations

This time-limited assessment focused exclusively on validating the reduction in attack surface achieved via compliance with the STIG - along with validating that the controls applied as part of the STIG were appropriately applied. It was not focused on identifying any platform vulnerabilities beyond confirming the intended reduction in attack surface.

Some controls contained within the STIG were unable to be tested by NCC Group as part of this assessment, but are expected to be covered by a separate Common Criteria Evaluation report that Google intends to publish alongside the release of Android 12. The details of this separate report are not discussed herein.

This evaluation only validated the controls as implemented by Google's Test DPC application, and did not make any judgment or assessment about third-party solutions that use these APIs and should themselves be independently validated.

Key Findings

With the full set of STIG requirements applied, the threats specified in the PPMDF were effectively mitigated. Of the individual STIG requirements reviewed, no issues were identified that impacted CAT I STIG requirements. The findings

[1] https://commoncriteriaportal.org/files/ppfiles/pp_md_v3.1.pdf

below pertain to CAT II and CAT III issues.

- The CAT II STIG requirement for password complexity did not appear to be correctly implemented in the version of Android 12 that was tested. It was expected (according to the STIG controls) that two repeated or sequential numbers would be rejected, however this rejection only seemed to happen if four numbers were repeated or sequential (see NCC-GOOG169-001). This is considered as a legacy requirement which is updated in the newer STIG and is not considered a risk due to other anti-brute force mitigations.
- The CAT III STIG control requires that the MDM be able to disable (among others) Wi-Fi functionality on the device. It was found during testing that even when disabled, it was possible for an authenticated user to enabled Wi-Fi through the 'Quick Settings' application.

Dashboard

Target Metadata

Name	Android 12

Engagement Data

Method	Black-box
Dates	2021-09-17 to 2021-10-04
Consultants	1
Level of Effort	10 person-days

Targets

Google Pixel 4A 5G

Finding Breakdown

Critical issues	0
High issues	0
Medium issues	0
Low issues	2
Informational issues	3
Total issues	**5**

Category Breakdown

Access Controls	1
Authentication	1
Other	3

Key

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. For an explanation of NCC Group's risk rating and finding categorization, see Appendix A on page 13.

Title	Status	ID	Risk
Passwords Permitted Containing Three Repeating or Sequential Characters	Fixed	001	Low
Wi-Fi Remains Configurable via Quick Settings	Fixed	005	Low
User Can Disable Authentication of Personal Hotspot Connections	Reported	002	Informational
Fingerprint Authentication Still Usable for Purchases and Application Authentication	Reported	003	Informational
Bluetooth Quick Toggle Functional When Bluetooth Disabled By MDM	Reported	004	Informational

Finding	**Passwords Permitted Containing Three Repeating or Sequential Characters**
Risk	**Low** Impact: Low, Exploitability: None
Identifier	NCC-GOOG169-001
Status	Fixed
Category	Authentication
Impact	A user can set a less complex PIN/Password than that mandated by the STIG.
Description	STIGID GOOG-12-006100 states: "*Google Android 12 must be configured to not allow passwords that include* ***more than two*** *repeating or sequential characters.*" The following prescribed procedure was followed: 1. Open "Lock screen" settings. 2. Open "Password constraints". 3. Set password quality to "Numeric (Complex)". Afterward, NCC Group noted that the following PINs were accepted by the device: • 333666 • 123321 This appears to fall outside of the specified boundary.
Recommendation	Validate whether there is an issue with the Test DPC application configuring the restriction correctly, or whether this is a bug.
Client Response	A revised procedure was suggested: 1. Open "Lock screen" settings. 2. Open "Password constraints". 3. Set password quality to "Numeric (Complex)". 4. Set password length to 6. 5. Tap "Request User to set a new password". then try to see if you can use repeating numbers or characters when setting the new password. However it was still possible to set the repeating and sequential PINs. **10/06/2021:** Google confirmed that the repeating number login in Android 12 is only hit at the 4th digit. A mitigation is being added to the STIG stating: "Does not Meet, can be mitigated by increasing the passcode length from 6 to 8 digits and selecting Medium or High complexity." **31/03/22:** Google observed that this is a legacy requirement that DISA is changing in the next STIG revision due to the fact that smartphones have strong anti-brute force measures such as throttling and triggering a factory reset of the device. As an example, the Samsung Android 12 STIG already incorporates this change. Consequently NCC Group no longer considered this an issue.
STIGID	GOOG-12-006100

Finding	**Wi-Fi Remains Configurable via Quick Settings**
Risk	**Low** Impact: Medium, Exploitability: Medium
Identifier	NCC-GOOG169-005
Status	Fixed
Category	Other
Impact	An attacker, or an indifferent or unaware user could configure the device to connect to an insecure Wi-Fi network, which could facilitate (for example), man-in-the-middle attacks.
Description	In the Test DPC application, there is a configuration option to "Disallow config Wi-Fi", with the expectation that this ensures the end-user cannot configure the Wi-Fi settings on the device. Although accessing Wi-Fi via `Settings -> Network and Internet -> Internet` resulted in the expected error:

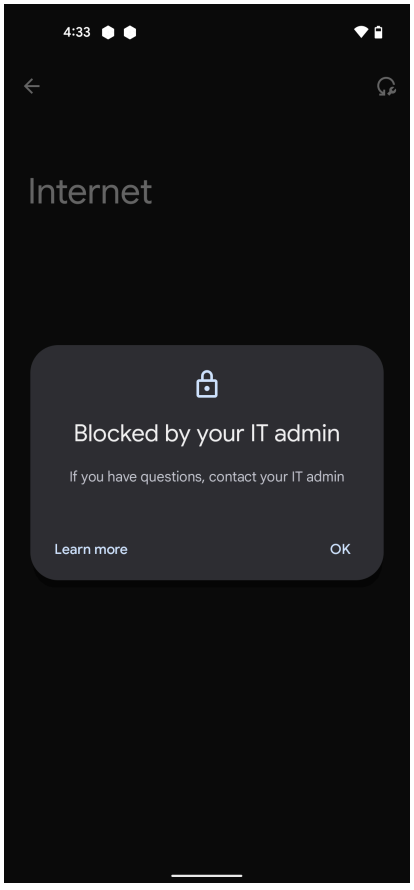

Figure 1: Expected denied message

It was observed however that Wi-Fi could still be configured by the extended quick menu panel:

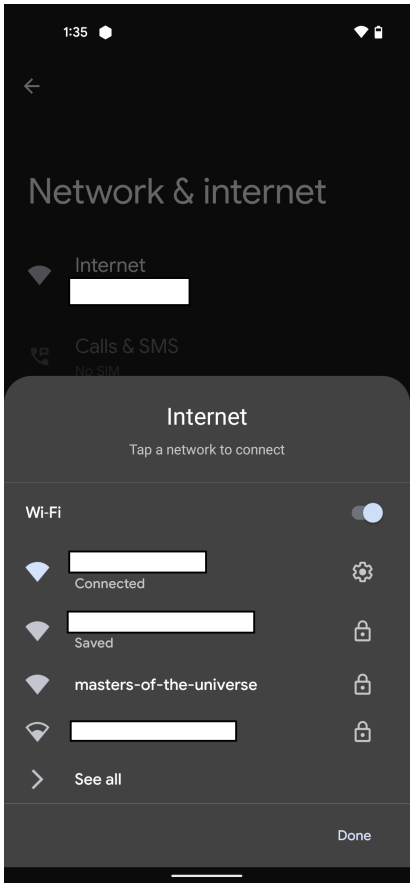

Figure 2: Wi-Fi quick menu

From this screen, it was possible to enable and disable Wi-Fi, and connect to new networks.

The STIG states that *"Google Android 12 must provide the capability for the Administrator (EMM) to perform the following management function: enable/disable the cellular radio, Wi-Fi radio, and Bluetooth radio (if the radio is supported by the mobile device)"*.

This has been rated as low risk for the following reasons:

- it would require a trusted user to unlock the device to make this configuration change
- the majority of applications on Android are now using TLS by default,[2] which mitigates the risk of connecting to an insecure Wi-Fi network
- the Android operating system requires use of certificates stored in the CA trust store (this is controlled and managed by Enterprise API, and therefore difficult to tamper with)
- the ability to disable Wi-Fi (among other radio interfaces), is a CAT III requirement (an additional mitigation, rather than a core enforcing function of confidentiality, availability or integrity)

Recommendation The Internet quick settings panel needs to be configured to respect the configuration option

[2] https://security.googleblog.com/2019/12/an-update-on-android-tls-adoption.html

	from TestDPC.
Client Response	Google noted that this issue had been identified in earlier testing, and is to be fixed in an upcoming security bulletin. **February 2022**: It was confirmed that this was addressed in the Android 12 December QPR Update
STIGID	GOOG-12-001200

Finding	**User Can Disable Authentication of Personal Hotspot Connections**
Risk	**Informational** Impact: None, Exploitability: Undetermined
Identifier	NCC-GOOG169-002
Status	Reported
Category	Access Controls
Description	STIGID GOOG-12-003400 states: *Google Android 12 must allow only the Administrator (MDM) to perform the following management function: enable/disable authentication of personal hotspot connections to the device using a preshared key.* STIGID GOOG-12-008700 states: *Google Android 12 must be configured to enable authentication of personal hotspot connections to the device using a preshared key.* Although the MDM *is* able to enable or disable the entire functionality of personal hotspot connections, it was not possible to control the authentication of personal hotspots connections. In policies where tethering is permitted, a user can remove the requirement to enter a preshared key (PSK) to join the hotspot. It was noted that the STIG guidance is that the personal hotspot (also referred to as tethering) functionality should remain disabled. For this reason, this is now raised for information only.
Reproduction Steps	• Open the Settings application. • Navigate to “Network & internet” -> “Hotspot & tethering” -> “Wi-Fi hotspot”, configure the “Security” option to “None”. • Validate that the hotspot for the device is available as an insecure WiFi network.
Recommendation	Address the requirement via the removal of the “Security” option on the “Wi-Fi hotspot” menu item.
STIGID	GOOG-12-003400, GOOG-12-008700

Finding	**Fingerprint Authentication Still Usable for Purchases and Application Authentication**
Risk	**Informational** Impact: None, Exploitability: None
Identifier	NCC-GOOG169-003
Status	Reported
Category	Other
Description	The STIG states: *Google Android 12 must allow only the Administrator (MDM) to perform the following management function: enable/disable authentication mechanisms providing user access to protected data other than a Password Authentication Factor, including [selection: biometric fingerprint, iris, face, voice, hybrid authentication factor).* It was observed when testing this requirement that, although it was possible for MDM to disable the biometric fingerprint functionality to unlock the test device, a user is still able to authenticate purchases and individual application access via fingerprint. This is raised for information only as the control is fundamentally meeting the requirement to control access to protected data (preventing unlocking of the device). In addition, is also stated elsewhere in the STIG that the biometric fingerprint is an approved authentication mechanism.
STIGID	GOOG-12-002100

Finding	**Bluetooth Quick Toggle Functional When Bluetooth Disabled By MDM**
Risk	**Informational** Impact: None, Exploitability: None
Identifier	NCC-GOOG169-004
Status	Reported
Category	Other
Description	It was noted that when Bluetooth was disabled via the TestDPC application, the Quick Settings button still appeared to turn Bluetooth on and off. However functionally, Bluetooth remained disabled. This is raised as informational user experience issue.
Recommendation	While NCC Group did not observe a security issue, it is recommended to review and correct this implementation.

Appendix A: 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.

Critical Implies an immediate, easily accessible threat of total compromise.

High Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.

Medium A difficult to exploit threat of large-scale breach, or easy compromise of a small portion of the application.

Low Implies a relatively minor threat to the application.

Informational 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.

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.

High Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.

Medium Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.

Low Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.

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.

High Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.

Medium Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.

Low Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

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.

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