



APP SECURITY ANALYSIS REPORT

Northcap

Napp v2.2.0

Document date: 09/19/2024

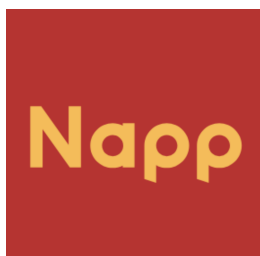


TABLE OF CONTENTS

1. HOW TO READ THE REPORT
2. EXPLORE BEYOND
3. DYNAMIC ANALYSIS: SUMMARY
4. EVIDENCES
5. SECURITY SCORE

STRICTLY CONFIDENTIAL

1. HOW TO READ THE REPORT

Each vulnerability is assigned a criticality score ranging from 0 to 10 based on the CVSS v3.1 standards. This score considers the ease of exploit implementation and the potential risk in case of a successful exploit. The score is then recalculated by factoring in parameters that account for the client's reputation, business, and policy areas. This results in a real risk score that accurately measures the level of risk. Based on the resulting score, the vulnerability is assigned a risk level, which is indicated in the table under the column "Range".

LEVEL	DESCRIPTION	RANGE
	No vulnerability	0
	Low vulnerability	0.1 – 3.9
	Medium vulnerability	4 – 6.9
	High vulnerability	7 – 8.9
	Critical vulnerability	9 – 10

Mobisec has come up with three risk flags that show when evidence, regardless of its score, is the result of a **bug**, when it might pose a **risk to the business**, and when it needs **special attention** because it could have a negative impact on compliance, best practices, market standards, or more.

Any personal, sensitive, or confidential data collected during testing may appear in dynamic analysis evidence.

This data will potentially be obfuscated using the following notation: ***.

All the vulnerabilities we have found are grouped according to the OWASP MASVS v2.1 standard.

MOBISec FLAGS



Bug



Business Risk



Caution

STANDARD MASVS

MASVS - STORAGE

MASVS - PLATFORM

MASVS - CRYPTO

MASVS - CODE

MASVS - AUTH

MASVS - RESILIENCE

MASVS - NETWORK

MASVS - PRIVACY

STRICTLY CONFIDENTIAL

2. EXPLORE BEYOND

We investigate the application from a unique perspective, exactly as an external hacker would do. This analysis reveals points of interest, vulnerabilities and strengths, providing a strategic advantage not available internally. This privileged view is critical to accurately and confidently address risks. This is essential to prevent, address and overcome cyber security challenges. An outside view to understand current vulnerabilities and anticipate future threats ensures an intelligent and proactive security path.

Our analysis

The application is natively developed in JAVA with the addition of external links that, by invoking the system browser, lead to the display of pages such as the privacy policy, FAQs, or the modification of personal data. Using this method to open links introduces risk boundaries related to the browser, which could be mitigated by using WebView, although the best option would still be to create native activities for the data management screens.

The app allows access to all the services offered by the company, such as digital payments, viewing recent purchases, geolocation using Google REST APIs, finding nearby points of interest, accessing new promotions, and inviting others to register.

All network communications take place through an HTTPS channel, with the app ensuring that the certificate is at least signed by a CA. REST APIs are primarily invoked using the GET method, while the POST method is used only for login, session token renewal, and entering promotional codes.

Payments through the app are handled with proprietary PayPal REST APIs, which manage both PayPal accounts and credit cards; the payment, made using a QR code and a token changed at each session, is further secured by server-side checks by PayPal for the presence of proxies, thus preventing, at least for this function, a potential Man-In-The-Middle (MITM) attack.

The filesystem is partially used correctly, as files and cache are properly encrypted. However, preference files are not protected by any encryption method, which could lead to the disclosure of sensitive information. It should be noted that the integrity of these data is ensured by a check that the application performs at each startup: if the files stored on the device do not match those on the server, they will be downloaded again.

The initial login is protected by a maximum attempt limit, which thwarts brute-force attacks, making the application less appealing for phishing or identity theft techniques.

Notes

STRICTLY CONFIDENTIAL

When attempting to use the **Recover Password** function, the message *"The email has been sent successfully"* is always returned, even when entering email addresses that are not present in the database. While this is a security advantage, as it prevents potential attackers from discovering which emails are in the database, we suggest considering a different and more realistic communication if the user enters an incorrect or non-existent email address.

3. DYNAMIC ANALYSIS: SUMMARY

The first column shows the evidence number in the risk analysis section. The second column shows the actual severity, indicated in the synopsis (SE), with the CVSS v3.1 score. The third column indicates the simplicity of possible exploit implementation (EX) on a scale of 1 to 4, with a higher value indicating greater difficulty of implementation.

ID	SE	EX	DETAILS
NAP-006	9.9	1	Authorization control is not implemented correctly and allows access to other users' data.
NAP-001	6.5	2	The application has no certificate pinning, so it is vulnerable to Man-in-the-Middle (MITM) attacks capable of reading and modifying data exchanged during communications.
NAP-002	5.5	2	Encryption of network communications is entrusted only by TLS. A MITM attack would compromise confidentiality and integrity of data in transit.
NAP-003	3.4	4	The certificate of the app is signed with SHA-1, a cryptographic hash function that has been defined as insecure since February 2017. Given this problem, there could be the possibility of an attacker signing the app by impersonating the same developer.
NAP-014	0	-	Security providers are not implemented properly.

4. EVIDENCES

VULN ID: NAP-006

MASVS-PLATFORM-1



Score 9.9

Critical vulnerability

Vector string

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L

Confidentiality

AT RISK

Integrity

AT RISK

Availability

AT RISK

Broken access control

There is no proper authorization control for access to resources. Some APIs only check the validity of the session to allow reading and writing of confidential data of other users. A registered app user could, in fact, query a REST API with a database of emails obtained from third parties, receive in response, the codes of customers registered with those emails that are actually in the database, and then query a second API to obtain all the information of the users whose codes they have obtained.

This issue could create a potentially massive data breach that would almost certainly lead to the intervention of the Privacy Authority and the imposition of a fine under GDPR regulations.

Request: GET https://domain.tld/app/1.0/getAnagrafica?comp=1&app=APP01&v=2.0.0&os=android&cliente=C999&codFIscale=AAAAAA00A00A000A

Response: [...], "cognome": "****", [...], "email": "****", [...], "nome": "****", "localita": "CARMAGNOLA", "via": "VIA ****", "numero_cellulare": "****", [...], "provincia": "TO", [...], "comune_nascita": "****", [...], "provincia_nascita": "TO", "sesso": "M"}

Possible remediation

Return only the data belonging to the user associated with the session authorization token. Identify the user based on the same token, not a query/API parameter.

STRICTLY CONFIDENTIAL

VULN ID: NAP-001

MASVS-NETWORK-1



Score 6.5

Medium vulnerability

Vector string

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

Confidentiality

AT RISK

Integrity

AT RISK

Availability

AT RISK

Lack of certificate pinning

The app has a security check that ensures the presence of a valid certificate on the server it communicates with, which prevents communication through self-signed proxies. However, if the server has a certificate issued by a trusted Certificate Authority (CA), it is seen as secure, which can allow Man-in-the-Middle (MITM) attacks to read any client-server network communication.

Domain: domain.tld

Possible remediation

Implement certificate pinning on the app (e.g., by introducing the server's public key into the code) allowing only Point-To-Point (P2P) communications between the device and the server, discarding any communication involving another device in between.

STRICTLY CONFIDENTIAL

VULN ID: NAP-002

MASVS-AUTH-1



Score 5.5	Medium vulnerability				
Vector string	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L				
Confidentiality	AT RISK	Integrity	AT RISK	Availability	AT RISK

Lack of E2E encryption

Certificate pinning significantly mitigates the risk of a MITM attack, capable of reading and modifying data in transit between the client and server. However, on compromised devices, it is possible to bypass the pinning and intercept communications through a proxy, allowing for sniffing and data injection into requests to the server, and altering the responses received by the client.

Request: POST https://domain.tld/sso/logincontroller

APPID=app123&userName=***&password=***

Possible remediation

Encrypt client-server communications with a session key generated during the app start-up using a key agreement protocol.

STRICTLY CONFIDENTIAL

VULN ID: NAP-003

MASVS-CRYPTO-1



Score 3.4	Low vulnerability				
Vector string	CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N				
Confidentiality	AT RISK	Integrity	AT RISK	Availability	OK

SHA-1 signed the app certificate

As announced by Google, in collaboration with CWI of Amsterdam, in February 2017 an internal failure of the SHA-1 function was discovered and a hash collision attack was carried out, whereby it was confirmed that two different pieces of data could generate the same digest. The fact that the app is signed with SHA-1 enables an attacker to make changes to publish a malicious app, impersonating a certified developer.

Algorithm: [SHA1withRSA]

Signature: -----

Possible remediation

Renewing the certificate by changing the signature algorithm would allow you to secure the deployment of the application. Otherwise, rely on the Google “App Bundle” service, which allows to send the application code to the Play Store and request that Google itself builds and signs the application.

STRICTLY CONFIDENTIAL

VULN ID: NAP-014

MASVS-NETWORK-1



Score 0

No vulnerability

MASTG-TEST-0023 - Misconfiguration with security provider

Updating the Security Provider in Android applications based on Google Play Services is critical for maintaining the security of HTTPS connections. If the ProviderInstaller is not invoked correctly or exceptions are not properly handled, the application remains vulnerable to SSL exploits.

GmsCore_OpenSSL security provider is not implemented properly.

Possible remediation

To mitigate the issue, it's necessary to correctly invoke the ProviderInstaller at the application's startup and handle exceptions to maintain an acceptable level of security. NDK applications must bind only to updated and secure SSL/TLS libraries.

STRICTLY CONFIDENTIAL

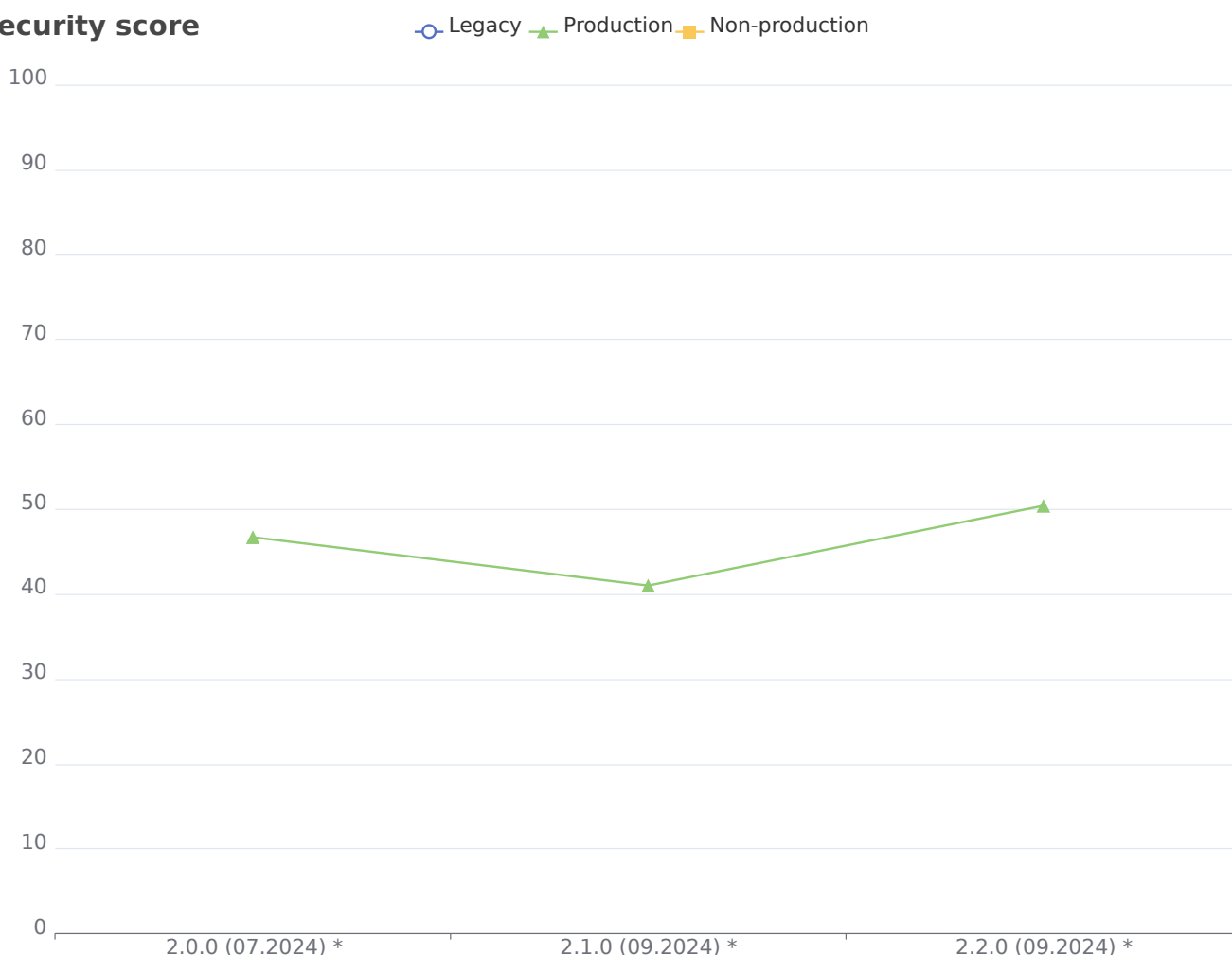
5. SECURITY SCORE

We have also put together a single security index that sums up all the vulnerabilities and security issues in the report. This application security index is a score between 0 and 100, where the higher the value, the better the security.

The difference between the *legacy* and newer scores is down to more testing and the way the results are broken down, which has changed the scale. It would be best to treat the previous *legacy* score as almost equal to the first point in the new data set. In any case, it is probably not a good idea to compare the *legacy* and newer data sets.

Security score: 50.4 /100

Security score



STRICTLY CONFIDENTIAL



THANK YOU

Mobisec Italia srl

Viale della Repubblica, 22
31020 Villorba (TV) – Italia

email: info@mobisec.com

P.Iva e C.F.
04735010268