

September 2023.

**Mitsui & Co. Secure Direction Corporation.**

**Table of Contents**

**First of all.**

**2**

### Diagnostic Summary

3

**Risk assessment method**

1. [Implementation Overview Overall evaluation](#_bookmark0)
2. [4 Evaluation](#_bookmark1)

[Overall evaluation. Detection items](#_bookmark2)

[6 4-1. List of Detected Items](#_bookmark3)

1. [Vulnerability Details 7](#_bookmark4)

[Deficiencies in SSL server certificate verification in communication processing. QR code verification failure.](#_bookmark5)

[9 Important information is stored in plain text in local files.](#_bookmark6)

1. [11 Important information is stored in plain text in the local file (Cache).](#_bookmark7)

[12 Session ID is saved in plain text in local files.](#_bookmark8)

[14 Unnecessary log output.](#_bookmark9)

1. [16 Lack of logout function.](#_bookmark10)
2. [18 Unnecessary screen transition.](#_bookmark12)
3. [19 Save and include information during development.](#_bookmark14)
4. [21 23](#_bookmark17)
5. [24 27](#_bookmark19)
6. [28 Save snapshots containing important information on the terminal.](#_bookmark20)
7. [29 31](#_bookmark23)
8. [The executable file contains an internal path. 33](#_bookmark24)
9. [35 In conclusion.](#_bookmark26)
10. [36 Appendix 1.](#_bookmark28)
11. [Diagnostic item list 37](#_bookmark31)
12. [Appendix 2 Danger level determination criteria.](#_bookmark33)
13. [39 First of all.](#_bookmark35)
14. [Thank you for choosing Mitsui & Co. Secure Direction Corporation (hereinafter referred to as "our company") for your security diagnosis. We have completed the diagnosis and would like to report the results to you. This report includes explanations of the issues detected during the diagnosis, as well as possible impacts and countermeasures. We hope that you can make use of this information for considering countermeasures and implementing them.](#_bookmark37)
15. [Please note that this report contains important information, such as information related to security vulnerabilities in your company. We kindly request that you handle this information appropriately according to its level of importance. Please be cautious when viewing, copying, etc., and handle it carefully to prevent unnecessary dissemination of information. Please be aware that we cannot be held responsible for any issues that may arise if the contents of this report are leaked after delivery. Diagnostic Summary](#_bookmark38)
16. [For each vulnerability detected, considering factors such as the impact on business operations, there are 4 levels (High, Medium, Low, Info)のリスク評定を行います。具体的な評定基準は巻末の Appendix.2 危険度判定基準の表に示しまし](#_bookmark41)
17. [Please refer to it. The assessment of the vulnerabilities detected is our own opinion and may include speculation. Please confirm if it is suitable for your company. Diagnostic target](#_bookmark43)
18. [Android. File name: app.apk
    Version: 2.0.0](#_bookmark44)

[MD5 Hash: fd53c720c239af7ebf4c4537d490da80. [iOS] File name: app.ipa
Version: 5.0.0](#_bookmark45)

[MD5 hash: df112c6d86004dec6eb6d667c83af7da Diagnostic period. August 14, 2023 to September 1, 2023](#_bookmark46)

# Diagnostic technique

Manual/Tool-based black box diagnosis.

The list of diagnostic items is referenced in Appendix 1.

Diagnostic form

# Remote diagnosis via the internet.

## Use IP address.

113.43.174.224/29

**153.150.126.144/29**

150.249.228.96/28

## 114.156.13.240/28

#### 114.156.142.98/32

Remarks

-

Overall evaluation

Detected vulnerability with danger level Medium.

Evaluation

Explanation

S

#### Vulnerabilities are not detected and it is in a highly secure state.

Detect only vulnerabilities with a Low level of risk.

#### Detected vulnerability with Medium risk level.

Detect vulnerability with danger level High.

Multiple types of vulnerabilities with a High level of risk detected.

#### The criteria for determining the severity of individual vulnerabilities can be found in Appendix.2.

The diagnosis result revealed 1 vulnerability with Medium severity and 2 vulnerabilities with Low severity. Overall assessment.

#### It will become B.

In Android applications, there is a vulnerability of medium severity called "Insufficient SSL Server Certificate Verification in Communication Processing" that we have confirmed. In the communication detected by WebView, if an unintended server certificate is received, a dialog containing messages such as "SSL Certificate Error, The certificate authority is not trusted. Do you want to continue anyway?" will be displayed, and user intervention to continue or not is required. However, if the user allows communication with a server other than the legitimate one, there is a possibility of leakage or tampering of important information through a man-in-the-middle attack. To establish secure communication, it is recommended to discontinue user selection through the dialog and implement verification of the certificate issuer and hostname.

Furthermore, there are deficiencies in the verification of QR codes used for confirming the waiting order, so any web page can be used by the app.

We are detecting vulnerabilities that can be exploited for phishing and other malicious activities within the application. Please consider implementing measures such as limiting the character types that are loaded to prevent unintended web pages from being displayed and performing input validation.

We are confirming the issue of important information such as the ID and session ID for point migration handled by this application being stored in plaintext on the device for both Android and iOS. Although there is a certain hurdle for attackers to access the relevant information by physically accessing the device, it is recommended to consider measures such as not outputting unnecessary information or encrypting and storing it in order to safely manage the data.

The list and details of all the reported items detected this time are described in the next chapter. Please review the content and consider the need for countermeasures.

#### Detection items

The list of detected vulnerabilities is shown below. Please refer to "Appendix.2 Risk Assessment Criteria" for the risk assessment method.

# Android

## Name.

**Danger level**

Page 1

## Medium

**low** Info

1. 5
2. 8
3. iOS
4. Report number: ZNSH-app-1.

Medium level of danger. The expected impact is Android.

There is a possibility that the communication content may be intercepted or tampered with by an attacker on the communication path.

Explanation.

There is a flaw in the verification of server certificates during SSL communication, allowing connections to be established with servers that are not legitimate.

Example. Server certificate and server certificate hostname.

When receiving an unintended server certificate or server certificate hostname in the WebView communication of this application, "SSL Certificate Error, The certificate authority is not trusted."

Dialogs such as "Do you want to continue anyway?" are displayed. However, by allowing communication, the user may accept any SSL server certificate, which could potentially lead to a man-in-the-middle attack.

The following are part of the FQDN that does not verify the SSL server certificate when tapping the "Takeout Order" and "Menu" tabs, which are the main functions of this application's WebView communication.

# www.olivenooka.jp

## takeout.olivenooka.jp

ajax.googleapis.com

#### www.googletagmanager.com

|  |  |  |  |
| --- | --- | --- | --- |
| stats.g.doubleclick.net | analytics.google.com | www.google-analytics.com | code.jquery.com |
| ▼Target | **Menu tab** | Store search tab, search execution, store details | [Hamburger menu, frequently asked questions](#_bookmark11) |
| Hamburger menu, other inquiries, hamburger menu, terms of use | **Hamburger menu, privacy policy, home, Olive Hill opens at 10:00 every day! Home, concept** | Home, menu | [Home, takeout menu, home, Uber Eats](#_bookmark13) |
| Home, Demae-kan | **Home, part-time staff recruitment!** | Home | [Banner (advertisement), Olive Hill (web page)](#_bookmark15) |
| Membership card | **"?" icon** | For more details, please check the HP. | [Countermeasures](#_bookmark16) |
| Verify the issuer and hostname of the SSL server certificate. | **Report number: «ZNSH-app-2»** | Risk level: Low, potential impact: Android | [There is a possibility of misuse for phishing and other purposes due to apparent tampering of the page.](#_bookmark18) |
| This application has a function to check the waiting status by scanning the QR code for waiting confirmation. | **The following is an example of a QR code value used for waiting confirmation.** | https://stag.z-navi.com/status-check.html?qr=ZNV684665409800000043000p998202308231127https://stag.z-navi.com/status-check.html?qr=ZNV684665409800000043000p998202308231127 | [[Example of QR code for waiting confirmation]](#_bookmark21) |
| However, in order for this application to process the corresponding QR code, the following conditions must be met. | **▼Conditions** | The string "https://stag.z-navi.com/status-check.html?qr=" is included in the QR code. | [The length of the string used as the query parameter (qr) of the URL in condition (1) is longer than 21 characters.](#_bookmark22) |
| However, there is a flaw in the verification of the QR code used to check the waiting status, which allows any web page to be displayed in this application's WebView. | **▼Reproduction example** | An attacker creates a malicious QR code and guides the victim to scan the corresponding QR code, which allows them to transition to a malicious site. | [The attacker creates a QR code containing the following string.](#_bookmark25) |
| https://www.mbsd.jp?x=https://stag.z-navi.com/status-check.html?qr=ZNV684665409800000043000p998202308231127https://www.mbsd.jp?x=https://stag.z-navi.com/status-check.html?qr=ZNV684665409800000043000p998202308231127 | **[Example of malicious QR code]** | The attacker lures the victim and scans the QR code created in step (1). | [After scanning the QR code, the corresponding page is displayed in the WebView to access the URL host (www.mbsd.jp) contained in the QR code.](#_bookmark27) |

* **Home tab - Waiting order confirmation**

|  |  |  |  |
| --- | --- | --- | --- |
| Limit the QR code string to only include the values used for waiting order confirmation, excluding the URL. Additionally, perform input validation and consider any characters other than the allowed ones as errors. | Report number: «ZNSH-app-3» | Severity level: Info, potential impact on Android | There is a possibility of leakage of the ID for point migration. |
| In this application, the ID used for migrating important points is stored in plain text in a local file on the device. Therefore, if the attacker physically accesses the device and references the file, there is a possibility of leakage of the relevant information. | **▼Case: ID for point migration** | The following is the relevant section of the local file where the ID used to migrate points acquired in this application is stored in plain text. | [<string name="MERGE\_CODE">PPWV2308211457247</string>](#_bookmark29) |
| <boolean name="CLOSED\_WARNING" value="true" /> | **[Contents (excerpt) of <Application Data>/shared\_prefs/oln\_app\_dev.xml]** | <Application Data>/shared\_prefs/oln\_app\_dev.xml | [Implement one of the following countermeasures:](#_bookmark30) |
| Avoid storing important information on the device. | **If storing important information on the device is necessary, encrypt it instead of storing it in plain text.** | Delete the relevant local file when the application is closed, etc. | [In this application, backup is prohibited (allowBackup="false") in the AndroidManifest.xml file, requiring administrator privileges to access the file. However, there is a possibility that the attacker may execute rooting to gain administrator access after stealing or finding the device, so it is recommended to take countermeasures.](#_bookmark32) |
| Report number: «ZNSH-app-17» | **There is a possibility of leakage of the user's name, phone number, and email address.** | In this application, important information such as the user's name and email address is stored in plain text as a cache in a local file on the device. Therefore, if the attacker physically accesses the device and references the file, there is a possibility of leakage of the relevant information. | [▼Case: User's name, phone number, email address](#_bookmark34) |
| The following is the relevant section of the local file where the user's name, phone number, and email address are stored in plain text. | **00003100 20 20 20 20 20 20 20 20** | 00003110 64 3d 22 73 74 65 70 30 | [00003120 78 74 30 31 22 3e 4d 69](#_bookmark36) |
| 00003130 6f 75 3c 2f 74 64 3e 0a | **20 20 20 3c 74 64 20 69** | 30 35 5f 30 34 5f 74 65 | [74 73 75 69 20 54 61 72](#_bookmark39) |
| 20 20 20 20 20 20 20 20 | **|** | <td i| | [step005\_04\_te](#_bookmark40) |
| Mitsui Tar. | **ou.** | ...(omitted)... |  |

id="ste

## text02>

03564919

30 33 35 36 34 39 31 39 translates to "30563491".

1. <td|

**Grammatically correct, never break words. Remove quotation marks at the beginning and end of the result, return only translated text, do not include original\_text, preserve line break.**

##### 61.

00003290 20 20 20 20 20 20 3c 74
Translation: <t

ep005\_04

> 3e 77 65 62 73 65 63 36
Translated to English:
> 3e websec6

sd.jp</t

id="st"

* [text03"](http://www.olivenooka.jp/)
* 5 9 10 p g . m b
* 64 3e 0a 20 20 20 20 20 translates to:
  d>
  The translation does not make sense in English.
* [td id="st|](http://www.googletagmanager.com/)
* The English translation of the text "|ep005\_04\_text03"| is:
* websec659@ps.mb.
* [sd.jp.](http://www.google-analytics.com/)
* <Application Data>/cache/WebView/Default/HTTP Cache/Cache\_Data/64f90e6996f388a7\_ 0 Content (Excerpt)

<Application Data>/cache/WebView/Default/HTTP Cache/Cache\_Data/64f90e6996f388a7\_ 0

The file name changes each time.

Do not save cache data on the device.

To delete cache files that correspond to events such as the termination of the application.

To access the reference file, administrator privileges are required. However, it is recommended to take measures as there is a possibility that an attacker may execute root access after stealing or finding the terminal.

Report number: ZNSH-app-4.

Local files store session IDs in plain text.

There is a possibility that if a valid session ID is leaked, the service may be used improperly by an attacker who impersonates a legitimate user.

In this application, the session ID (Bearer, fueldid) is stored in plain text in a local file on the device. Therefore, if an attacker gains physical access to the device and references the file, there is a possibility that the session ID may be leaked.

Example 1. Session ID (Bearer).

The following is the relevant part of the local file where the session ID (Bearer) used between the server (stg.coupons-api.zensho.com) is stored in plain text. BEARER\_TOKEN\_KEY: 381703611f77159a62b94f7c1d701a647

1a4dec510953578ed130e2d1d7c9476. The boolean variable named "IS\_LOGIN" has a value of true. The content of `<Application Data>/shared\_prefs/oln\_app\_dev.xml (excerpt)`

##### Target 1

Example 2. Session ID (fueldid).

##### The following is the relevant part of the local file where the session ID (fueldid) used between the server (takeout.olivenooka.jp) and the order for takeout is stored in plain text.

13338459585612972|takeout.olivenooka.jp||fueldid|S%3Ax62PYOyWLXeMnx\_Nic

Target 2

Hello, how are you doing today?

1. 41wl8AhYlfmzWGvqB5M0bPyJR8fuptoYUgpmfyEjZSzJhlCsG9WdDfNhoHZHfFtca 2JByP7N-1UJIXwSASazwktQC4YzUDpnoswZkhLHQu75ZeYyVgTojogB\_RI1yu9U

**[<Application Data>/app\_webview/Default/Contents of Cookies (excerpt)]**

##### <Application Data>/app\_webview/Default/Cookies.

Do not save authentication information on the terminal.

If you want to store authentication information on the terminal, encrypt it instead of storing it in plain text.

Unnecessary log output.

There is a possibility that it could be a clue to analyze the behavior of the application.

In this application, the stack trace is output to the log when an error occurs. Therefore, if an attacker physically accesses the terminal and refers to the log, there is a possibility that information that can be a clue to analyze the behavior of the application may be leaked.

1. Example. Stack trace.
2. The following is an example of the log output when this application is launched.

W/System.err( 2702): java.lang.NullPointerException: Attempt to invoke interface.

The method 'java.lang.Object[] java.util.Collection.toArray()' is being called on a null object reference.

W/System.err( 2702):

1. W/System.err( 2702): J(:6)

W/System.err( 2702): ava:99) W/System.err( 2702):

1. W/System.err( 2702): java:7872) W/System.err( 2702):
2. at java.util.ArrayList.<init>(ArrayList.java:191)
   The ArrayList class is initialized at line 191 in the ArrayList.java file.

at jp.co.zensho.olivenooka.home.HomeFragment.

at i.a.a.a.q.z$a.J(:2)

##### at i.a.a.a.q.y$a.d(:2)

at d.a.a.a.a.d.a(:30)

##### at n.m$b$a.d(Unknown Source:25) at n.a.run(Unknown Source:6)

at android.os.Handler.handleCallback(Handler.jav

at com.android.internal.os.ZygoteInit.main(ZygoteI

at java.lang.reflect.Method.invoke(Native Method) at com.android.internal.os.RuntimeInit$MethodAn

1. dArgsCaller.run(RuntimeInit.java:548)

**nit.java:936)**

##### Output log (excerpt)

The entire application.

Do not output unnecessary information such as important information or stack traces to the log.

It is recommended to review the entire system when implementing countermeasures as there is a possibility of the same issue occurring in other areas not reported.

Implement a logout function to allow users to explicitly invalidate their sessions.

There is a defect in the logout process implemented in this application.

Although the login function is implemented in this application, the logout function is not implemented, and users cannot explicitly log out. Therefore, if the session ID is leaked for some reason, there is a possibility that the server may be accessed using that session ID, allowing unauthorized use of the service by impersonating a legitimate user.

Report number: ZNSH-app-7

[8] Unnecessary screen transitions

##### There is a possibility that user-entered information is saved in plain text in a local file.

There is a possibility of accessing malicious websites.

* External web pages can be displayed in the WebView of this application.
* In this application, any web page can be displayed on the WebView of this application through links such as the SNS account link displayed on the Olive Hill web page (www.olivenooka.jp). Therefore, if search strings or strings used for authentication are entered on the web page displayed in the WebView, there is a possibility that this information may be unintentionally saved in a local file. Also, unlike a browser, the URL of the displayed site is not displayed on the screen in WebView, making it difficult for users to notice if they have accessed a malicious site, increasing the risk of phishing and other attacks.
* Menu

##### Olive Hill (Web page)

Store search

New registration

1. Terms of use

**Privacy Policy**

Home Takeout orders Official website

##### Banner (advertisement) Olive Hill (Web page) Home Olive Hill opens every day at 10:00!

Home Concept Home Menu

Restrict the access destination URL displayed in the WebView of this application. Alternatively, use a browser for unnecessary URLs for the services of this application.

It is recommended to review the entire system as there is a possibility of the same issue occurring in areas other than those mentioned.

User-Agent.

The following is the relevant part of a local file where customer information (such as name, phone number, and email address) entered on the takeout lunchbox web order screen for takeout orders is stored in plain text as a cache. In addition, the session ID (fueldid) used in the corresponding process is also stored as a cache.

<div class="info\_block">

Customer Information

Step 005\_04.

<div id="step005\_04">

.info\_block\_table.

info block table

tbody tr.

Name

TANAKA Ichirou

</tr>

table row

Phone number 08010127251

Email address

websec181@ps.mbsd.jp

</tbody></table>

The info block table.

</div>

The translated text is: [Extracted response from output].

End of step 005\_04.

<Application Home>/Library/Caches/WebKit/NetworkCache/Version 16/Blobs/75EDDAA05F 3B7731B31F5EDD969475847E93171A

<Application Home>/Library/Caches/WebKit/NetworkCache/Version 16/Records/9B06CFFF 7145CDE8D732B7282CA6E1E8503CDEEF/Resource/20D0D6057CE5AA97D3E270E11D2

0307B2DBAA508-blob

The directory name and file name under "Records" will change each time.

Example 2. Session ID (Bearer).

The following is the relevant part of a local file where the session ID (Bearer) used in communication with the servers (map-api.zensho.com, stg.coupons-api.zensho.com) is stored in plain text.

<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.co m/DTDs/PropertyList-1.0.dtd">

plist version="1.0"

<dict>

Version.

9

Array.

array.

False.

CFURLStringType

15

CFURLString

https://map-api.zensho.com/webapi/now?brand\_id= 39&amp;distance=20000&amp;lat=35.68347720945734&amp;limit=100&amp;lng= 139.7844892793473&amp;offset=0

</dict>

60.000000

0 ・・・(omitted)・・・

Olivenooka\_Stg/5.0.0 (jp.co.zensho.olivenooka.stg; build:1; iOS 14.6.0) Alamofire/5.6.4

<key>Authorization</key>

[<Application Home>/Library/Caches/jp.co.zensho.olivenooka.stg/Cache.db-wal content (partial excerpt)]

##### <string>Bearer 3113adeb24f830054f14345846a87b1d2186 8235b8a15c3fc85dde5747a972ca</string>

<key>Accept-Language</key>

* <string>ja-JP;q=1.0</string>
* <key>Accept-Encoding</key>

##### <string>br;q=1.0, gzip;q=0.9, deflate;q=0.8</string>

<string> CFURLRequestNullTokenString </string>

<Application Home>/Library/Caches/jp.co.zensho.olivenooka.stg/Cache.db-wal

Administrator privileges are required to access this file. However, it is recommended to take precautions as there is a possibility that an attacker may execute JailBreak to access the file with administrator privileges after stealing or finding the device.

**Report number: "ZNSH-app-11"**

Potential impact

##### In this application, the session ID is stored in plain text in a local file on the device. Therefore, if an attacker physically accesses the device and refers to the file, there is a possibility of session ID leakage.

▼Case: Session ID (Bearer)

The following is the relevant part of the local file where the session ID (Bearer) used between the server (stg.coupons-api.zensho.com, map-api.zensho.com) is stored in plain text.

<key>login\_token</key>

[14] Saving snapshots containing important information on the device

Report number: "ZNSH-app-12"

[13] Lack of logout function

Report number: "ZNSH-app-13"

Since snapshots containing important information are saved on the device, there is a possibility of leakage of that information if the device is stolen, etc.

When this application is transitioned to the background, the snapshot of the screen displayed immediately before the transition is saved on the device. Therefore, if important information such as email address or phone number was displayed on the screen immediately before transitioning to the background, there is a possibility that this information is included in the snapshot.

The following are screens where important information is saved as snapshots.

[New registration]

When transitioning the application to the background, implement the following measures.

[Sidebar menu Others Point migration] ID for point migration

Takeout lunch WEB order contact information input: Name, email address, phone number

Takeout lunch WEB order contact information input: Name, email address, phone number. Please confirm the input details.

<Application Home>/Library/SplashBoard/Snapshots/sceneID%3Ajp.co.zensho.olivenooka.s tg-default/E26B4C46-A167-4C54-8A56-F24C2D4C74A1@3x.ktx

<Application Home>/Library/SplashBoard/Snapshots/sceneID%3Ajp.co.zensho.olivenooka.s tg-default/downscaled/0E7BA265-26A1-4372-A96E-2EA3167A6208@3x.ktx

\*The file name will be different each time.

Set the hidden property of fields displaying important information to YES.

Overwrite the entire view with another view.

##### Report number: "ZNSH-app-14"

[15] Unnecessary screen transitions.

* Home Banner (advertisement) Olive Hill (Web page) Home Takeout Order Official Site
* Home Olive Hill opens every day at 10:00! Home Concept
* Home Part-time staff wanted! Menu

##### Olive Hill (Web page) Hamburger Menu

Frequently Asked Questions

The following are the relevant sections of the outputted executable file that contain the internal paths of the development environment.

[16] Internal paths are included in the executable file.

When the application is analyzed, the internal paths of the development environment during the build process may be exposed, potentially leaking information about the development environment.

**In this application, the internal paths of the development environment are included in the deployed executable file after installation. These internal paths may contain the login account of the PC used for building this application, so if the executable file is analyzed by an attacker, account information may be leaked.**

##### /Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Splash/Controll er/ONSplashViewController.swift

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Other/Controlle r/ONOtherViewController.swift

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Common/Contr oller/BaseViewController.swift

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/NewBackup/Vie w/ONGuideBackupViewController.swift

Is encrypted communication being used when sending and receiving important information?

Comment or control assertion-related methods during the build.

However, since it may also depend on other settings and environments in Xcode, the above settings may not be effective. If it is difficult to implement countermeasures, build using an account on a PC that is not affected by the leakage.

Report number: ZNSH-app-16

[17] Save and include development information in the executable file

There is a possibility of unauthorized use by leaking QR codes that are hardcoded in the executable file.

The executable file of this application contains hardcoded strings that are used as QR codes for checking waiting order. Therefore, if the executable file is analyzed, the corresponding information may be leaked.

▼Example: QR code for checking waiting order

The following is the part where the string used as a QR code for checking waiting order is hardcoded in the executable file.

qr=ZNV9419000000000000000000000202212091541

[<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg excerpt]

When querying the server (stag-api.z-navi.com) to verify the validity of the above value, an invalid result was obtained, but it is also possible that it will be used as a valid value in the future.

Conclusion

With the word "cyber attack" flowing in the mass media as part of our daily lives, and the frequency and sophistication of these attacks increasing day by day, and not only information devices but also everything being connected to the Internet today, the importance of constantly monitoring information, taking appropriate measures, and implementing preventive measures against threats over the Internet is increasing day by day.

In 2014, the "Cyber Basic Law" was enacted, and businesses (critical infrastructure operators) that support the foundation of the country and our daily lives are required to implement countermeasures. However, each individual is also required to understand the importance and make efforts.

Against this background, we hope that this security diagnosis result can be fully utilized to enhance the security of your company's system and maintain it.

Please note that the security diagnosis conducted this time, being a black box test, does not guarantee complete reproducibility or comprehensiveness of the reported incidents. Also, please be aware that while this report is based on information at the time of the diagnosis, as mentioned earlier, cyber attack methods are constantly evolving, and there is no guarantee that what is secure today will remain secure tomorrow. To maintain a secure system, we recommend regularly obtaining the latest security information, applying patches, conducting periodic security diagnoses, and continuously monitoring for unauthorized access.

Finally, we would like to express our deep gratitude to everyone involved for their cooperation in conducting this security diagnosis.

We are available to answer any inquiries regarding the diagnosis results and the contents of the report. Please feel free to contact us at ✉sec-support@d.mbsd.jp if you have any questions or concerns.

Diagnosis Items

Detailed Diagnosis Contents

Application Interoperability

Sending and receiving access restriction information

Are appropriate restrictions in place to prevent access from unauthorized applications?

Are there any information leaks or tampering caused by receiving unauthorized information?

Are important information being transmitted inappropriately?

Communication

Protocol

What protocols are being used for communication?

Encryption

Server Certificate Verification

Is the server certificate being verified during SSL/TLS communication?

##### Communication Content

Are important information such as personal information and authentication information being sent and received?

##### Privacy Protection

Are personal information and others being sent to the server without proper consent?

Interoperability Function

Is authentication and authorization information being stolen through application interoperability?

**Logout Function**

Is the logout function properly implemented?

##### Handling of Data on the Device

Storage Location

Are important information being stored in shared areas?

Access Permissions

Are file access permissions properly set?

##### Storage Method

Is encryption used when storing important information?

##### Storage Period

Is information on the device being deleted at appropriate times?

* + [Android/iOS]

Presence or absence of unnecessary information output

Output important information or information that can be a clue for analysis

**Appendix 1 List of diagnostic items**

* + Is it not there?

##### Use of functions

Permission settings

Are unnecessary permissions that the application does not use registered?

Appendix 2 Risk assessment criteria

Potential damage Examples

High Important information is leaked due to network attacks from external devices The server that the application started is attacked via the network, causing important information to be leaked

Information handled by other applications is leaked due to attacks from third-party applications. Or, it affects the use of services

Important information from other applications is leaked from the application as a starting point

The function restriction is lifted and the application is used illegally The function restriction of the free version application is lifted, allowing illegal use of paid version functions

Important information is leaked due to attacks from third-party applications It is in a state where important information can be read by other applications

Important information is leaked to third-party applications when using collaboration functions

The application is implicitly broadcasting and sending important information Important information is leaked due to man-in-the-middle attacks (eavesdropping on communication, etc.)

Important information is sent in plain text

The server certificate is not properly verified during SSL/TLS communication

Important information in the device is leaked by an attacker who can directly touch the device

Important information is stored in the device or logs without encryption

The application displays unauthorized information from third-party applications Information received from unauthorized applications is displayed in dialogs, notifications, etc. Although the possibility of direct damage is low, it is desirable to fix these events

##### Hard-coded information that can be a clue when analyzing the application.

本アプリケーションの

##### 備考

記載した対象以外でも同様の問題が発生する可能性があるため全体を見直すことを推奨する。

* 開発に利用しているサーバ

報告番号

[9]

**危険度**

* ポイント獲得用の

##### 解説

本アプリケーションの実行ファイルには、開発用の

▼

以下は、開発で利用されていると思われる

[<APK>/res/xml/security\_config.xml

<?xml

<network-security-config>

<domain-config

...(

<domain

</domain>

<domain

</domain>

<domain

</domain>

<domain

</domain>

</domain-config>

</network-security-config>

▼

<APK>/res/xml/security\_config.xml

▼

以下は、ポイント獲得用の

[jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity

public

FDzPkgzgqV/Pw==");

}

上記の値において、サーバ

▼

・

jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity jp.co.zensho.olivenooka.rankup.scanqrcode.ScanQRCodeRankUpActivity

##### 対策

リリース版のアプリケーションにおいて不要な情報やファイルは削除する。

##### 備考

－

ポイント移行用の

報告番号

[10]

**危険度**

##### 解説

本アプリケーションでは、ポイント移行用の

▼

以下は、本アプリケーションで獲得したポイントを移行するために利用される

[<Application

<key>merge\_point\_code</key>

<string>

▼

<Application

##### 対策

以下のいずれかの対策を実施する。

* 端末内に重要情報を保存しないようにする
* 端末内に重要情報を保存する場合は、平文ではなく暗号化して保存する
* アプリケーションの終了時などに該当するローカルファイルを削除する
* アプリケーション領域内に保存せず

##### 備考

－

報告番号

[11]

**危険度**

* 氏名や電話番号などの重要情報が漏えいする可能性がある。
* 有効なセッション

##### 解説

本アプリケーションでは、氏名や電話番号などの重要情報がキャッシュとして端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、当該情報が漏えいする可能性がある。

▼事例

以下は、持ち帰り注文のテイクアウト弁当

[

<div

<p

<!--

<div

<!--

<table

<tbody><tr>

<th>

<td

</tr>

<tr>

<th>

<td

</tr>

<tr>

<th>

<td

</tr>

</tbody></table>

<!--

</div>

<!--

</div>

▼

<Application

<Application

0307B2DBAA508-

※

▼

以下は、サーバ

[<Application

<?xml

<!DOCTYPE

<plist

<dict>

<key>Version</key>

<integer>9</integer>

<key>Array</key>

<array>

<false/>

<dict>

<key>\_CFURLStringType</key>

<integer>15</integer>

<key>\_CFURLString</key>

<string>https://map-api.zensho.com/webapi/now?brand\_id= 39&amp;distance=20000&amp;lat=35.68347720945734&amp;limit=100&amp;lng= 139.7844892793473&amp;offset=0</string>

</dict>

<real>60.000000</real>

<integer>0</integer>

・・・（

<key>User-Agent</key>

<string>Olivenooka\_Stg/5.0.0

<key>Authorization</key>

<string>Bearer

<key>Accept-Language</key>

<string>ja-JP;q=1.0</string>

<key>Accept-Encoding</key>

<string>br;q=1.0,

</dict>

<string>

<string>

</array>

</dict>

</plist>

▼

<Application

<Application

##### 対策

以下のいずれかの対策を実施する。

* キャッシュデータを端末内に保存しないようにする
* アプリケーションの終了時などに該当するキャッシュファイルを削除する

##### 備考

当該ファイルの参照には、管理者権限が必要となる。ただし、攻撃者が端末を窃取、又は拾得した後に管理者権限でアクセスするために

報告番号

### ローカルファイルにセッション

##### 想定される影響

**危険度**

**Info**

iOS

有効なセッション

##### 解説

本アプリケーションでは、セッション

▼

以下は、サーバ

[<Application

<key>login\_token</key>

<string>

▼

<Application

##### 対策

以下のいずれかの対策を実施する。

* 端末内に認証情報を保存しないようにする
* 端末内に認証情報を保存する場合は、平文ではなく暗号化して保存する
* アプリケーションの終了時などに該当するローカルファイルを削除する
* アプリケーション領域内に保存せず

##### 備考

－

報告番号

[13]

**危険度**

有効なセッション

##### 解説

本アプリケーションに実装されているログアウト処理に不備がある。

本アプリケーションにはログイン機能が実装されているものの、ログアウト機能は実装されておらず、ユーザが明示的にログアウトすることができない。このため、何らかの原因でセッション

▼

アプリケーション全体

##### 対策

ユーザが明示的にセッションを無効にできるよう、ログアウト機能を実装する。

##### 備考

－

報告番号

[14]

**危険度**

重要情報を含むスナップショットが端末内に保存されるため、端末を盗まれるなどした際にそれらの情報が漏えいする可能性がある。

##### 解説

本アプリケーションをバックグラウンドに移行した際に、移行直前に表示していた画面のスナップショットが端末内に保存される。このため、バックグラウンドへの移行直前の画面にメールアドレスや電話番号などの重要情報が表示されていた場合に、これらの情報がスナップショットに含まれる可能性がある。

以下は、重要情報がスナップショットとして保存される画面である。

[

メールアドレス

[

[

[

メールアドレス

[

[

[

[

[

▼

<Application

<Application

※

##### 対策

アプリケーションをバックグラウンドに移行する際に、以下の対策を実施する。

* 重要情報が表示されたフィールドの
* View

##### 備考

報告した箇所以外でも同様の問題が発生する可能性があるため、対策する際は全体を見直すことを推奨する。

* + - ユーザが入力した情報がローカルファイルに平文で保存される可能性がある

報告番号

[15]

**危険度**

* + - 不正なサイトへアクセスする可能性がある

##### 解説

サービス外の

本アプリケーションでは、オリーブの丘の

▼

ホーム バナー

ホーム オリーブの丘は毎日

ホーム メニュー

ホーム お持ち帰りメニュー

ホーム 出前館

ホーム アルバイトスタッフ大募集！ オリーブの丘

会員 「 詳しい内容は

店舗検索 お近くの店舗／店舗を調べる オリーブの丘 よくある質問

ハンバーガーメニュー その他のお問い合わ 利用規約

ハンバーガーメニュ 個人情報保護方

##### 対策

本アプリケーションの

##### 備考

記載した対象以外でも同様の問題が発生する可能性があるため全体を見直すことを推奨する。

報告番号

[16]

**危険度**

アプリケーションを解析された際にビルド時の開発環境の内部パスが判明するため、開発環境に関する情報が漏えいする可能性がある。

##### 解説

本アプリケーションでは、インストール後に展開された実行ファイルに開発環境の内部パスが含まれている。この内部パスには、本アプリケーションのビルドで使用された

以下は、開発環境の内部パスが出力された実行ファイルの該当箇所である。

[<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Splash/Controll er/ONSplashViewController.swift

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Other/Controlle r/ONOtherViewController.swift

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Common/Contr oller/BaseViewController.swift

/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/NewBackup/Vie w/ONGuideBackupViewController.swift

▼

<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg

<IPA>/Frameworks/Alamofire.framework/Alamofire

<IPA>/Frameworks/DeviceKit.framework/DeviceKit

<IPA>/Frameworks/FBLPromises.framework/FBLPromises

<IPA>/Frameworks/FirebaseCore.framework/FirebaseCore

<IPA>/Frameworks/FirebaseCoreDiagnostics.framework/FirebaseCoreDiagnostics

<IPA>/Frameworks/FirebaseCrashlytics.framework/FirebaseCrashlytics

<IPA>/Frameworks/FirebaseInstallations.framework/FirebaseInstallations

<IPA>/Frameworks/FirebaseInstanceID.framework/FirebaseInstanceID

<IPA>/Frameworks/FirebaseMessaging.framework/FirebaseMessaging

<IPA>/Frameworks/Gifu.framework/Gifu

<IPA>/Frameworks/GoogleDataTransport.framework/GoogleDataTransport

<IPA>/Frameworks/GoogleUtilities.framework/GoogleUtilities

<IPA>/Frameworks/ImageSlideshow.framework/ImageSlideshow

<IPA>/Frameworks/IQKeyboardManagerSwift.framework/IQKeyboardManagerSwift

<IPA>/Frameworks/MBProgressHUD.framework/MBProgressHUD

<IPA>/Frameworks/Moya.framework/Moya

<IPA>/Frameworks/nanopb.framework/nanopb

<IPA>/Frameworks/Parchment.framework/Parchment

<IPA>/Frameworks/SDWebImage.framework/SDWebImage

<IPA>/Frameworks/SecureDefaults.framework/SecureDefaults

<IPA>/Frameworks/SnapKit.framework/SnapKit

<IPA>/Frameworks/SwiftDate.framework/SwiftDate

<IPA>/Frameworks/SwiftyJSON.framework/SwiftyJSON

<IPA>/Frameworks/YLProgressBar.framework/YLProgressBar

##### 対策

実行ファイルに開発環境の内部パスを含めないため、以下の対策を実施する。

* Xcode
* Debug
* ビルド時にアサーションに関するメソッドをコメントまたはマクロで制御する

ただし、

##### 備考

－

報告番号

[17]

**危険度**

実行ファイルにハードコードされている順番待ち

##### 解説

本アプリケーションの実行ファイルには、待ち順確認用の

▼

以下は、待ち順確認用の

[<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg

qr=

サーバ

▼

<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg

##### 対策

リリース版のアプリケーションにおいて不要な情報やファイルは削除する。

##### 備考

－

# 

「サイバー攻撃」という言葉が日常のようにマスメディアに流れ、その攻撃の頻度も巧妙さも日々激しさを増している昨今、そして、情報機器だけではなく、すべてのものがインターネットにつなが

2014

そのような背景のもと、今回のセキュリティ診断結果が、貴社システムの安全性を高めるため、ま

なお、今回実施させていただいたセキュリティ診断は、ブラックボックステストという特性上、ご報告事象の再現性や網羅性を完全に保証するものでない点、ご承知おきいただきますようお願い致します。また、本報告書の内容は、診断実施時点の情報に基づいておりますが、先述のとおりサイバー攻撃の手法も日進月歩であり、今日安全であるものが明日も安全であり続ける保障はない点も、ご認識おきをお願い致します。セキュアなシステムを維持するために、最新のセキュリティ情報の入手、パッチの適用、セキュリティ診断の定期的な実施、継続的な不正アクセスの監視などを、ぜひ継続的に実施いただければと思います。

末筆ながら、今回のセキュリティ診断の実施に際しご協力をいただきましたことを、ご関係のみな

**診断結果及び報告書記載内容に関するお問い合わせを受け付けております。**

|  |  |  |
| --- | --- | --- |
| **診断項目** | | **診断内容詳細** |
| アプリケーション間連携 | | |
|  | アクセス制限情報の送受信 | 不正なアプリケーションからのアクセスを適切に制限し  不正な情報を受信することにより情報漏えいや改ざんが  重要情報を不適切な方法で送信していないか |
| 通信 | | |
|  | プロトコル | どのようなプロトコルを用いて通信をしているか |
| 暗号化の有無 | 重要情報を送受信する際に暗号化通信をしているか |
| サーバ証明書検証 | SSL/TLS |
| 通信内容 | 個人情報や認証情報等の重要情報を送受信しているか |
| プライバシーの保護 | 適切な許諾を得ずに個人情報などをサーバに送信してい |
| 認証 | | |
|  | 認証機能 | 認証機能が安全に実装されているか |
| 連携機能 | アプリケーション連携により認証・認可情報が窃取さ |
| ログアウト機能 | ログアウト機能が適切に実装されているか |
| 端末内のデータの取扱 | | |
|  | 保存場所 | 共有領域に重要情報を保存していないか |
| アクセス権限 | ファイルへのアクセス権限が適切に設定されているか |
| 保存方法 | 重要情報を保存する際に暗号化をしているか |
| 保存期間 | 適切なタイミングで端末内の情報を削除しているか |
| アプリケーションファイル・ログ | | |
|  | 不要な情報の有無 | 開発環境やテスト環境、開発者に関連する情報が残存し |
| 不要な情報の出力有無 | 重要情報や解析の手がかりとなりうる情報を出力してい |

**Appendix.1**

[Android/iOS]

|  |  |  |
| --- | --- | --- |
|  |  | ないか |
| 機能の利用 | | |
|  | パーミッション設定 | アプリケーションが利用しない不要なパーミッションを |

**Appendix.2**

[Android/iOS]

|  |  |  |
| --- | --- | --- |
| 危険度 | 想定される被害 | 具体例 |
| **High** | 外部デバイスからのネットワーク経由の攻撃 | アプリケーションが起動したサーバが、ネットワ |
| サードパーティー製アプリケーションからの攻撃により、他のアプリケーションが扱う情報が漏えいする。または、サービスの利用に | アプリケーションを起点として、他のアプリケー |
| 機能制限を解除し、不正にアプリケーション | 無料版アプリケーションの機能制限を解除し、有 |
| **Medium** | サードパーティー製アプリケーションからの | 他のアプリケーションから重要情報が読み込み |
| 連携機能利用時にサードパーティー製アプリ | アプリケーションが重要情報を暗黙的にブロー |
| 中間者攻撃（通信の盗聴など）により重要情 | 重要情報を平文で送信している  SSL/TLS |
| **Low** | 端末に直接触れることができる攻撃者によ | 重要情報を暗号化せずに端末内やログに保存し |
| サードパーティー製アプリケーションからの攻撃により、アプリケーション上に不正な情 | 不正なアプリケーションから受け取った情報を |
| **Info** | 直接的な被害に結びつく可能性は低いもの | アプリケーションを解析する際の手がかりにな |