

[5] Session IDs are saved in plaintext in local files.

**Risk Level Info Expected Impact Android**

**Report Number: "ZNSH-app-4"**

**[5] Session ID is stored in plaintext in local files**

**Risk Level Info Expected Impact Android**

### If a valid session ID is leaked, there is a possibility that an attacker impersonating a legitimate user may illegally use the service.

Explanation

**In this application, the session ID (Bearer, fueldid) is stored in plaintext in local files on the device. Therefore, if an attacker physically accesses the device and references the file, there is a possibility of the session ID being leaked.**

1. [▼Case 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 plaintext.](#_bookmark0)
2. [<string name="BEARER\_TOKEN\_KEY">381703611f77159a62b94f7c1d701a647 1a4dec510953578ed130e2d1d7c9476</string>](#_bookmark1)

[<boolean name="IS\_LOGIN" value="true" /> <string name="BEARER\_TOKEN\_KEY">381703611f77159a62b94f7c1d701a647](#_bookmark2)

[1a4dec510953578ed130e2d1d7c9476</string> <boolean name="IS\_LOGIN" value="true" />](#_bookmark3)

1. [[Content of <Application Data>/shared\_prefs/oln\_app\_dev.xml (excerpt)] ▼Target 1](#_bookmark4)

[<Application Data>/shared\_prefs/oln\_app\_dev.xml ▼Case 2: Session ID (fueldid)](#_bookmark5)

[The following is the relevant part of the local file where the session ID (fueldid) used when placing a takeout order with the server (takeout.olivenooka.jp) is stored in plaintext. 13338459585612972|takeout.olivenooka.jp||fueldid|S%3Ax62PYOyWLXeMnx\_Nic](#_bookmark6)

1. [C1jv8YeExcTbPk0HXMxA%3D||/|13338466785612972|0|0|13338459585612972|1| 1|1|-1|2|443|0|13338459585613134 13338459579694626|takeout.olivenooka.jp||lat[0]|35.6852807||/|133410515796946](#_bookmark7)

[07|0|0|13338459579694626|1|1|1|-1|2|443|0|13338459579694626 AOeKKH-GFZJS\_GMcp07VTgj622sSwmDOOD7QlXyD49hflBemhv6RYrEPekUyS](#_bookmark8)

[41wl8AhYlfmzWGvqB5M0bPyJR8fuptoYUgpmfyEjZSzJhlCsG9WdDfNhoHZHfFtca 2JByP7N-1UJIXwSASazwktQC4YzUDpnoswZkhLHQu75ZeYyVgTojogB\_RI1yu9U 13338459585612972|takeout.olivenooka.jp||fueldid|S%3Ax62PYOyWLXeMnx\_Nic](#_bookmark9)

1. [C1jv8YeExcTbPk0HXMxA%3D||/|13338466785612972|0|0|13338459585612972|1| 1|1|-1|2|443|0|13338459585613134 13338459579694626|takeout.olivenooka.jp||lat[0]|35.6852807||/|133410515796946](#_bookmark10)
2. [07|0|0|13338459579694626|1|1|1|-1|2|443|0|13338459579694626 AOeKKH-GFZJS\_GMcp07VTgj622sSwmDOOD7QlXyD49hflBemhv6RYrEPekUyS](#_bookmark12)
3. [41wl8AhYlfmzWGvqB5M0bPyJR8fuptoYUgpmfyEjZSzJhlCsG9WdDfNhoHZHfFtca 2JByP7N-1UJIXwSASazwktQC4YzUDpnoswZkhLHQu75ZeYyVgTojogB\_RI1yu9U [<Application Data>/app\_webview/Default/Extract of Cookies]](#_bookmark14)
4. [▼Target 2 <Application Data>/app\_webview/Default/Cookies](#_bookmark17)
5. [Countermeasures Implement one of the following countermeasures.](#_bookmark19)
6. [Do not save authentication information on the device. If saving authentication information on the device, encrypt it instead of storing it in plain text.](#_bookmark20)
7. [Delete relevant local files when the application is closed. Remarks](#_bookmark23)
8. [- Report Number: «ZNSH-app-5»](#_bookmark24)
9. [[6] Unnecessary log output Severity Info Expected Impact Android](#_bookmark26)
10. [Report Number: «ZNSH-app-5» [6] Unnecessary log output](#_bookmark28)
11. [Severity Info Expected Impact Android It may provide clues for analyzing the behavior of the application.](#_bookmark31)
12. [Explanation In this application, the stack trace is output to the log when an error occurs. Therefore, if an attacker physically accesses the device and refers to the log, there is a possibility that information that can be a clue for analyzing the behavior of the application may be leaked.](#_bookmark33)
13. [▼Example: Stack Trace The following is an example of a log output when this application is launched.](#_bookmark35)
14. [W/System.err( 2702): java.lang.NullPointerException: Attempt to invoke interface method 'java.lang.Object[] java.util.Collection.toArray()' on a null object reference W/System.err( 2702):](#_bookmark37)
15. [W/System.err( 2702): J(:6) W/System.err( 2702):](#_bookmark38)
16. [W/System.err( 2702): W/System.err( 2702):](#_bookmark41)
17. [W/System.err( 2702): W/System.err( 2702):](#_bookmark43)
18. [W/System.err( 2702): a:942) W/System.err( 2702): ava:99) W/System.err( 2702):](#_bookmark44)

[W/System.err( 2702): W/System.err( 2702): java:7872) W/System.err( 2702): W/System.err( 2702):](#_bookmark45)

[at java.util.ArrayList.<init>(ArrayList.java:191) at jp.co.zensho.olivenooka.home.HomeFragment. at i.a.a.a.q.z$a.J(:2)](#_bookmark46)

# 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 android.os.Handler.dispatchMessage(Handler.j

## at android.os.Looper.loopOnce(Looper.java:201) at android.os.Looper.loop(Looper.java:288)

at android.app.ActivityThread.main(ActivityThread.

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

dArgsCaller.run(RuntimeInit.java:548)

## W/System.err( 2702):

#### nit.java:936)

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

W/System.err( 2702): java.lang.NullPointerException: Attempt to invoke interface method 'java.lang.Object[] java.util.Collection.toArray()' on a null object reference

ファイル名：

MD5

W/System.err( 2702):

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

W/System.err( 2702):

#### W/System.err( 2702):

W/System.err( 2702):

#### W/System.err( 2702):

W/System.err( 2702):

W/System.err( 2702): a:942)

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

W/System.err( 2702):

#### W/System.err( 2702): java:7872) W/System.err( 2702):

W/System.err( 2702):

at java.util.ArrayList.<init>(ArrayList.java:191)

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 android.app.ActivityThread.main(ActivityThread.

**at android.os.Looper.loopOnce(Looper.java:201) at android.os.Looper.loop(Looper.java:288)**

at java.lang.reflect.Method.invoke(Native Method) at com.android.internal.os.RuntimeInit$MethodAn dArgsCaller.run(RuntimeInit.java:548)

## W/System.err( 2702):

**nit.java:936)** at com.android.internal.os.ZygoteInit.main(ZygoteI

1. [Output log (excerpt)]
2. ▼Target
3. Entire application
4. Countermeasure

Do not output unnecessary information such as important information and stack traces to logs.

Remarks

It is recommended to review the entire application when implementing countermeasures, as similar issues may occur in places other than those reported.

Report number: "ZNSH-app-6"

[7] Lack of logout function

Severity Info Expected impact Android

Report number: "ZNSH-app-6"

[7] Lack of logout function

# Severity Info Expected impact Android

## If a valid session ID is leaked, there is a possibility that the service may be used illegally by an attacker who impersonates a legitimate user.

Explanation

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

|  |  |  |  |
| --- | --- | --- | --- |
| Although this application has a login function, it does not have a logout function, and users cannot explicitly log out. Therefore, if a session ID is leaked for some reason, it is possible for the server to be accessed using that session ID, allowing an attacker to impersonate a legitimate user and use the service illegally. | ▼Target | Entire application | Countermeasure |
| Implement a logout function to allow users to explicitly invalidate their sessions. | **Remarks** | - | [Report number: "ZNSH-app-7"](#_bookmark11) |
| [8] Unnecessary screen transitions | **Severity Info Expected impact Android** | Report number: "ZNSH-app-7" | [[8] Unnecessary screen transitions](#_bookmark13) |
| Severity Info Expected Impact Android | **There is a possibility that user-entered information will be saved in plain text in a local file.** | There is a possibility of accessing malicious websites. | [Explanation](#_bookmark15) |
| It is possible to display web pages outside of the service on the WebView of this application. | **In this application, any web page can be displayed on the WebView of this application from links such as SNS accounts 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 on the WebView, there is a possibility that this information will 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, so users may not notice that they have accessed a malicious site, and there is a possibility of being a victim of phishing, etc.** | ▼Target | [Menu](#_bookmark16) |
| Olive Hill (web page) | **Store search** | Nearby stores / Check stores | [Olive Hill (web page) Hamburger menu Frequently Asked Questions](#_bookmark18) |
| Hamburger menu Other inquiries Hamburger menu Terms of use | **Hamburger menu Privacy policy First startup Terms of use** | New registration | [Terms of use](#_bookmark21) |
| New registration | **Privacy policy** | Home Takeout order Official website | [Home](#_bookmark22) |
| Banner (advertisement) Olive Hill (web page) Home Olive Hill opens at 10:00 every day! | **Home Concept Home Menu** | Home Takeout menu Home Uber Eats | [Home Demae-can](#_bookmark25) |
| Home Part-time staff wanted! | **Membership card** | "?" icon | [Please check the website for more details.](#_bookmark27) |

* **Countermeasures**

|  |  |  |  |
| --- | --- | --- | --- |
| Restrict the access destination URL displayed on the WebView of this application. Alternatively, use a browser for unnecessary URLs for this application's service. | Remarks | It is recommended to review the entire system as there is a possibility of similar issues occurring outside the mentioned targets. | Report number: «ZNSH-app-8» |
| [9] Saving and including development information | **Severity Info Expected Impact Android** | Report number: «ZNSH-app-8» | [[9] Saving and including development information](#_bookmark29) |
| Severity Info Expected Impact Android | **There is a possibility of unauthorized access to the server (development environment) used for development.** | There is a possibility of unauthorized use by leaking QR codes for point acquisition. | [Explanation](#_bookmark30) |
| The execution file of this application contains hard-coded development IP addresses and QR codes for point acquisition. As a result, if the execution file is analyzed and the relevant information is leaked, there is a possibility of unauthorized access or misuse. | **▼Case 1: Development IP addresses** | The following is the relevant section of the file that stores information about IP addresses that are likely used in development. | [<?xml version="1.0" encoding="utf-8"?>](#_bookmark32) |
| <network-security-config> | **<domain-config cleartextTrafficPermitted="true">** | ...(omitted)... | [<domain includeSubdomains="true">52.68.217.122](#_bookmark34) |
| </domain> | **<domain includeSubdomains="true">54.64.74.199** | </domain> | [<domain includeSubdomains="true">54.64.59.18](#_bookmark36) |
| </domain> | **<domain includeSubdomains="true">3.115.201.116** | </domain> | [</domain-config>](#_bookmark39) |
| </network-security-config> | **<?xml version="1.0" encoding="utf-8"?>** | <network-security-config> | [<domain-config cleartextTrafficPermitted="true">](#_bookmark40) |
| ...(omitted)... | **<domain includeSubdomains="true">52.68.217.122** | </domain> | [<domain includeSubdomains="true">54.64.74.199](#_bookmark42) |

</domain>

## <domain includeSubdomains="true">54.64.59.18

▼Target 1

</domain-config>

1. </network-security-config>

**[Excerpt from <APK>/res/xml/security\_config.xml]**

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

▼Case 2: QR codes for point acquisition

The following is an example of the relevant section in the execution file where the hard-coded string used as a QR code for point acquisition is located in the class jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity.

public /\* synthetic \*/ void t0(View view) { l0("RJPQvq+qEwbkHDaIhkB4F8esLND83PxbDz2NtTh+B9fw+Q=OySqH38Pm

FDzPkgzgqV/Pw==");

}

* [public /\* synthetic \*/ void t0(View view) { l0("RJPQvq+qEwbkHDaIhkB4F8esLND83PxbDz2NtTh+B9fw+Q=OySqH38Pm](http://www.olivenooka.jp/)
* FDzPkgzgqV/Pw==");
* }
* [[Excerpt from jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity]](http://www.googletagmanager.com/)
* In the above values, it is possible that even though the results were invalid when queried to the server (stg.coupons-api.zensho.com), they may be used as valid values in the future.
* ▼Target
* [・APK file (class)](http://www.google-analytics.com/)
* jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity jp.co.zensho.olivenooka.rankup.scanqrcode.ScanQRCodeRankUpActivity

Countermeasure

Remove unnecessary information and files in the released version of the application.

Remarks

－

Report number: ZNSH-app-9.

[10] Important information is stored in plaintext in local files.

Low level of risk, impact on iOS is expected.

Report number: ZNSH-app-9

[10] Important information is stored in plaintext in local files.

Low level of risk, impact on iOS is expected.

There is a possibility of leakage of the ID used for point migration. Explanation

In this application, the ID used for point migration is stored in plaintext in a local file on the device. Therefore, if an attacker physically accesses the device and references the file, there is a possibility that the information may be leaked. ▼Example: 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 plaintext.

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

<string>PUDJ2308091602017</string>

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

<string>PUDJ2308091602017</string>

If storing important information on the device, encrypt it instead of storing it in plaintext.

Countermeasures

1. Implement one of the following countermeasures:

**Do not store important information on the device.**

##### Delete the relevant local file when the application is closed, etc.

Store it in the keychain instead of the application area.

Remarks

Report number: ZNSH-app-10

[11] Important information is stored in plaintext in local files (Cache).

Low level of risk, impact on iOS is expected.

1. Report number: ZNSH-app-10
2. [11] Important information is stored in plaintext in local files (Cache).

Low level of risk, impact on iOS is expected.

There is a possibility of leakage of important information such as name and phone number.

If a valid session ID is leaked, there is a possibility that an attacker impersonating a legitimate user may illegally use the service.

1. Explanation

▼Example 1: Name, phone number, session ID, etc.

1. The following is the relevant section of the local file where customer information (name, phone number, email address) entered on the takeout lunch web order screen for takeout orders is stored in plaintext as a cache. In addition, the session ID (fueldid) used in the relevant process is also stored as a cache.
2. <div class="info\_block">

<p class="info\_block\_title">Customer Information</p>

<!-- #step005\_04 -->

##### <div id="step005\_04">

<!-- .info\_block\_table -->

##### <table class="info\_block\_table">

<tbody><tr>

</tr>

<tr>

1. <th>Phone Number</th>

**<td id="step005\_04\_text02">08010127251</td>**

##### <tr>

<th>Email Address</th>

<td id="step005\_04\_text03">websec181@ps.mbsd.jp</td>

</tr>

<p class="info\_block\_title">Customer Information</p>

</div>

<div class="info\_block">

<!-- #step005\_04 -->

<div id="step005\_04">

##### <!-- .info\_block\_table -->

<table class="info\_block\_table">

* <tbody><tr>
* <th>Name</th>
* <td id="step005\_04\_text01">TANAKA Ichirou</td>

##### </tr>

<tr>

<tr>

1. <th>Email Address</th>

**<td id="step005\_04\_text03">websec181@ps.mbsd.jp</td>**

</tr>

##### </tbody></table>

<!-- /.info\_block\_table -->

</div>

[Extracted Response]

Severity

<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>

・・・（omitted）・・・

<key>User-Agent</key>

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

<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>

</dict>

<string> CFURLRequestNullTokenString </string>

<string> CFURLRequestNullTokenString </string>

</array>

</dict>

</plist>

<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>

</dict>

<string> CFURLRequestNullTokenString </string> <string> CFURLRequestNullTokenString </string>

</array>

</dict>

</plist>

▼Target 2

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

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

Countermeasure

Implement one of the following countermeasures.

Do not save cache data on the device.

Delete cache files when the application is closed.

Remarks

Administrator privileges are required to access the file. However, it is recommended to take precautions as attackers may execute JailBreak to gain administrator access after stealing or finding the device.

Report number: ZNSH-app-11

Session ID is stored in plaintext in local files. Potential impact

Info

iOS

If a valid session ID is leaked, an attacker impersonating a legitimate user may illegally use the service.

##### Explanation

In this application, the session ID is stored in plaintext in local files on the device. Therefore, if an attacker physically accesses the device and references the file, there is a possibility of session ID leakage.

* ▼Example: Session ID (Bearer)
* The following is the relevant section 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 plaintext.

##### <key>login\_token</key>

<string>3113adeb24f830054f14345846a87b1d21868235b8a15c3fc85dde5747a97 2ca</string>

▼Target

<Application Home>/Library/jp.co.zensho.olivenooka.stg.plist

**Countermeasures**

Implement one of the following countermeasures:

##### Do not save authentication information on the device.

If saving authentication information on the device, encrypt it instead of storing it in plaintext.

Delete relevant local files when the application is closed.

Store in keychain instead of saving in the application's area.

Report number: ZNSH-app-12

[13] Lack of logout function

Severity: Info

Potential impact: iOS

[13] Lack of logout function

Severity: Info

Potential impact: iOS

If a valid session ID is leaked, an attacker impersonating a legitimate user may illegally use the service.

Severity: Info

-

Report number: "ZNSH-app-13"

[14] Save snapshots containing important information on the device

Severity: Info

Report number: "ZNSH-app-13"

[14] Save snapshots containing important information on the device

Since snapshots containing important information are saved on the device, there is a possibility that this information may be leaked if the device is stolen, etc.

Explanation

##### 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 addresses or phone numbers is displayed on the screen immediately before transitioning to the background, there is a possibility that this information may be included in the snapshot.

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

* [New Registration]
* Email address
* [New Registration Email Address Verification] Email address

##### [New Registration Email Address Verification Register Profile] Gender, residential area

[Login]

Target

[Sidebar Menu Others Point Migration] ID for point migration

[Takeout Lunch Web Order Enter Contact Information] Name, email address, phone number

**[Takeout Lunch Web Order Enter Contact Information Confirm Input] Name, email address, phone number**

##### <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 is different each time.

Countermeasure

[<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg extracted string (excerpt)]

Olive Hill (web page) Hamburger menu

Frequently Asked Questions

Hamburger menu

Other inquiries Hamburger menu

Terms of use

Hamburger menu

Privacy policy

Countermeasures

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

Remarks

It is recommended to review the entire system as similar issues may occur in areas other than those mentioned.

Report number: ZNSH-app-15

[16] Internal paths are included in the executable file

Severity Info, Potential impact on iOS

Report number: ZNSH-app-15

[16] Internal paths are included in the executable file

Severity Info, Potential impact on iOS

There is a possibility of leaking information about the development environment when the application is analyzed and the internal path of the development environment at the time of building is determined.

Explanation

In this application, the internal path of the development environment is included in the deployed executable file after installation. This internal path 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.

The following are the relevant parts of the outputted internal path in the executable file.

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

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

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

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

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

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

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

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

Target

<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/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

* + Set -DNDEBUG=1 to the other\_c\_flags in Xcode's build options.

<IPA>/Frameworks/YLProgressBar.framework/YLProgressBar

Countermeasures

**To avoid including the internal path of the development environment in the executable file, implement the following countermeasures.**

* + Build with Release instead of Debug.

##### Comment or control the methods related to assertions during the build using comments or macros.

However, there may be cases where the above settings may not be effective as they depend on other configurations and environments in Xcode. If it is difficult to implement countermeasures, it is recommended to build using a PC account that does not have any impact if leaked.

Remarks

-

Report Number: "ZNSH-app-16" [17] Save and include development information

Severity Info, Potential impact on iOS Report Number: "ZNSH-app-16" [17] Save and include development information

Severity Info, Potential impact on iOS

There is a possibility of unauthorized use through the leakage of QR codes that are hard-coded in the executable file.

Explanation The executable file of this application contains hard-coded strings that are used as QR codes for checking waiting order. Therefore, if the executable file is analyzed, there is a possibility of leakage of relevant information.

▼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 hard-coded in the executable file.

qr=ZNV9419000000000000000000000202212091541

qr=ZNV9419000000000000000000000202212091541 [<IPA>/Olivenooka\_Stg.app/Olivenooka\_Stg content (excerpt)]

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

▼Target

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

Countermeasure

Remove unnecessary information and files in the released version of the application. Remarks -

##### Conclusion

With the word "cyber attack" flowing in the mass media as part of our daily lives, and the frequency and sophistication of such attacks increasing day by day, today where everything is connected to the internet, it is becoming increasingly important to constantly monitor information about threats over the internet, take appropriate measures, and implement preventive measures.

##### In 2014, the "Cybersecurity Basic Act" was enacted, and it is mandatory for businesses (critical infrastructure operators) that support the foundation of the country and our daily lives to implement countermeasures. However, it is also required for each individual to understand its importance and make efforts.

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

* Application Interoperability

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**

* Sending and receiving access restriction information

##### Properly restricting access from unauthorized applications

Ensuring no information leakage or tampering occurs through the receipt of unauthorized information

Ensuring important information is not sent inappropriately

Communication

Are there any remaining development or test environment-related information?

Ensuring that authentication and authorization information is not stolen through application collaboration

Logout function

Ensuring the proper implementation of the logout function

Handling of data within the device

Storage location

Not storing important information in shared areas

Access permissions

Ensuring that file access permissions are properly set

Storage method

Encrypting important information when storing

Storage period

Are you deleting information from the device at the appropriate timing?

Application files and logs

Presence of unnecessary information

Presence of unnecessary information output

Outputting important information or clues for analysis

Diagnostic items

Detailed diagnostic content

Protocol

Are there no information leaks or tampering due to receiving unauthorized information?

Are you not sending important information in an inappropriate manner?

Communication

What protocol are you using for communication?

Presence of encryption

Are you using encrypted communication when sending and receiving important information?

Server certificate verification

##### Are you verifying the server certificate during SSL/TLS communication?

Communication content

##### Are you sending and receiving important information such as personal information and authentication information?

Privacy protection

Logout function

Is the authentication function implemented securely?

Interconnectivity function

**Is authentication and authorization information not being stolen through application interconnectivity?**

##### Is the logout function properly implemented?

Handling of data within the device

Storage location

Are you not storing important information in shared areas?

Storage period

Storage method

Are you encrypting when storing important information?

Are you deleting information from the device at the appropriate timing?

Application files and logs

##### Presence of unnecessary information

Are there no remaining development or test environment-related information?

* Presence of unnecessary information output
* Outputting important information or clues for analysis
* Appendix.1 List of diagnostic items
* Appendix.1 List of diagnostic items

##### [Android/iOS]

Does not exist

Appendix.2 Hazard Assessment Criteria

Appendix.2 Hazard Assessment Criteria

**Hazard Level**

* Expected Damage
* Specific Examples

##### High

Leakage of important information due to network attacks from external devices

The server on which the application is running is attacked via the network, resulting in the leakage of important information

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

Info

Specific Examples

High

Leakage of important information due to network attacks from external devices

The server on which the application is running is attacked via the network, resulting in the leakage of important information

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

Leakage of important information from other applications as a result of the application being compromised

Unauthorized use of the application by removing functionality restrictions

Unlocking the functionality restrictions of the free version application and illegally utilizing the features of the paid version.

Medium

Leakage of important information due to attacks from third-party applications.

The application is in a state where important information can be read by other applications.

Leakage of important information to third-party applications when using collaboration features.

The application is implicitly broadcasting important information.

Leakage of important information due to man-in-the-middle attacks (eavesdropping on communication).

Sending important information in plain text.

Failure to properly verify server certificates during SSL/TLS communication.

Low

Leakage of important information in the device due to attackers who can directly access the device.

Storing important information in the device or logs without encryption.

Displaying unauthorized information on the application due to attacks from third-party applications.

Displaying information received from unauthorized applications in dialogs or notifications.

[Android/iOS].

</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 |