Phishing Google Wallet and Paypal by abusing WhatsApp

Update: 25.10.2013

CVE number for this issue has been assigned.

CVE: CVE-2013-6274

Introduction

WhatsApp is one of the most common used tools aka 'Apps' on Smarphone-Devices with access to wireless networks or a so called Data-'Flatrate'. By using the internet link to communicate, people do not have to pay any extra fees for sending a text-message somewhere, even if the receiver is in another country.

WhatsApp is available for almost every architecture on the market. The program exists for Nokia, Blackberry, Android and iOS. It is available here: https://www.whatsapp.com. This post will focus on the version for android.

The app is free for one-year in Android devices. After that time the user has to buy a yearly license. The application provides 3 methods of payment:

- google wallet
- paypal
- payment link.

They can be selected via Menu->Settings->Account->Payment Info.

Bug

Google-wallet and Paypal payments work in the same way. When selecting it, WhatsApp opens an in-app browser and contacts its main server www.whatsapp.com with the request:

```
/payments/google.php?phone=XXXXXXXXXXX&cksum=<request
checksum>&sku=1&lg=en&lc=US
```

or

```
/payments/paypal.php?phone=XXXXXXXXXXX&cksum=<request
checksum>&sku=1&lg=en&lc=US
```

Responding to this request the browser gets redirected to the proper checkout service.
The payment link option seems to be currently not working, i.e., nothing happens.

Attacks

Even tough the communication with the payment systems is HTTPS secured, the initial contact with the main server www.whatsapp.com is **NOT,** as we can see in Wireshark logs:

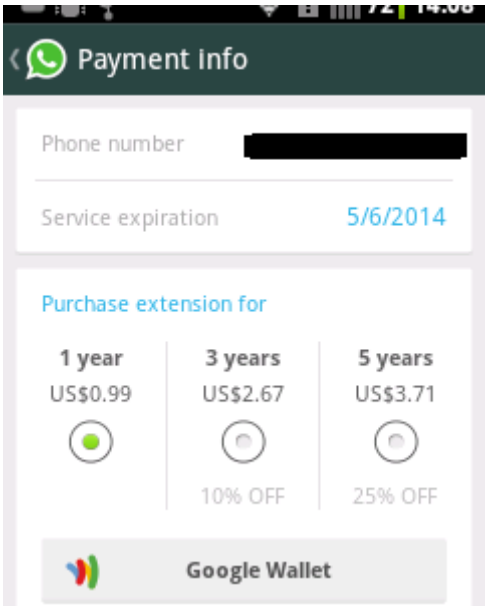
```
GET /payments/google.php?phone=xxxxxxxxxx&cksum=<checksum>&sku=1&lg=en&lc=US
HTTP/1.1
Host: www.whatsapp.com
Accept-Encoding: gzip
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7;
Cookie: __utmmobile=0xxxxxxxxxxxxxx
Accept:application/xml,application/xhtml+xml,text/html;
q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
```

After Whatsapp sent this unencrypted request, it will receive the following answer.

```
HTTP/1.1 200 OK
X-Powered-By: PHP/5.4.7
Content-type: text/html
Transfer-Encoding: chunked
Date: Mon, 10 May 2013 5:34:36 GMT
Server: lighttpd/1.4.31
5e4

<html>
<head>
<meta name="HandheldFriendly" content="true"/>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WhatsApp Messenger payment</title>
</head>
<body onLoad="document.getElementById('google').submit()">
<p>Please wait...</p>
<form id="google" method="POST" action="https://checkout.google.com
api/checkout/v2/checkoutForm/Merchant/xxxxxxxxxxxxxx" accept-charset="utf-8">
<input type="hidden" name="shopping-cart.items.item-1.item-name" value="One year of
WhatsApp service for phone XXXXXXXXXXXXXXX"/>
<input type="hidden" name="shopping-cart.items.item-1.item-description" value="WhatsApp
Messenger"/>
<input type="hidden" name="shopping-cart.items.item-1.merchant-item-id" value="1"/>
<input type="hidden" name="shopping-cart.items.item-1.merchant-private-item-data"
value="XXXXXXXXXXXXXXX"/>
<input type="hidden" name="shopping-cart.items.item-1.unit-price" value="0.99"/>
<input type="hidden" name="shopping-cart.items.item-1.unit-price.currency" value="USD"/>
<input type="hidden" name="shopping-cart.items.item-1.quantity" value="1"/>
<input type="hidden" name="shopping-cart.items.item-1.digital-content.display-disposition"
value="OPTIMISTIC"/>
<input type="hidden" name="shopping-cart.items.item-1.digital-content.email-delivery"
value="true"/>
<input type="hidden" name="checkout-flow-support.merchant-checkout-flow-support.continue-
shopping-url" value="http://www.whatsapp.com/payments/success.php"/>
<input type="hidden" name="_charset_" />
</form>
</body>
</html>
0
```

In your android phone this procedure usually looks like this:



Payment Information – Whatsapp

This is the screen to choose for the payment method. After clicking Google Wallet in this example normally you will see something like this:

However, in our case we do a redirect to our company webpage 😀

et voilà!

Curesec Webpage – Forwarding via Whatsapp

This means an attacker could intercept the first request via a suitable man-in-the-middle attack and successfully redirect the user to any Webpage when the user is trying to buy Whatsapp credit. To gain useraccounts the attacker could setup a fake Google-Wallet or Paypal Systems page to harvest user accounts. It might even be possible to gather directly money through this, for instance let the user pay the 0,99 cents via Google Wallet or Paypal to the account of the attacker.

Besides an attacker could forward some other content like a webpage with a new apk necessary for using google-wallet or paypal, like the (in)-famous Zitmo Trojan did at visiting a Bankingsite and spending users some extra "Security"-Features.

Practical abuse of the bug

As buying the credit only happens one time per year the attack itself is quite uncommon to be practical for a huge misuse as the attacker needs to be in control of the wireless or gsm network to intercept and redirect the traffic. On the other hand, in times of BYOD, open conference hotspots and big campus wireless networks it might be still very valueable for attackers.

Affected Versions

2.9.6447 to 2.10.751 (latest as of 2013 July 2)

Contact with Vendor History

19.06.2013	1st Mail from crt
19.06.2013	2nd Mail from crt
15.07.2013	3rd Mail – Send full bugdescription

No response.