my.eir.ie
HTTP Traffic and Exposed API

Summary

The my.eir.ie website contains a number of recently detected security vulnerabilities potentially allowing a malicious actor to gather information about multiple Eir customers or access the account of a single Eir customer.

Background

Corrata's mobile endpoint protection service detects and blocks HTTP POSTs from Apple iOS and Android devices to Internet servers. The canonical POST contains user entered data that is generally unadvisable to send unencrypted, such as login credentials.

This protection was triggered on 23/03/2023 by one of our end-users on the my.eir.ie website.
Corrata investigated this incident. This document presents our findings.

This is not a security audit. Our primary concern was to evaluate the correctness of the alert we received. We merely documented what we found while doing so.

All issues presented can be readily discovered using only the Web Developer tools available in all major browsers.

Vulnerabilities

Summary

1 . Bill notification email directs the user to an http site
2 . Insecure login page
3 . Unprotected GraphQL web service

➢ *Vulnerability 1. Bill notification email directs the user to an http site*

The eir bill notification email directs the user to view their bill at http://my.eir.ie/login, or to find help at http://support.eir.ie/bill/mybillexplained. Note the http links.

This is true of both the text/plain and text/html versions.

```
Your new eir bill is now available to view at my eir
<http://my.eir.ie/login>.

Your bill amount is *€ 44.44*

Once you login to my eir, you can view and download a PDF of your bill, pay
a bill and much more.

If you are set up for Direct Debit we will automatically take your payment.
If not, you can set up Direct Debit at any time in my eir.
If you need help understanding your bill we have a full bill explanation
available here <http://support.eir.ie/bill/mybillexplained>.
```

```
<tr>
<td style="font-family:Helvetica,arial,sans-serif;font-size:24px;text-align:left;line-
height:26px">
                                    eir bill notification</td>
</tr>
<tr>
```

<td width="100%" height="5" style="font-size:1px;line-height:1px">

</td>

</tr>

<tr>

<td height="20" style="font-size:1px;line-height:1px"> </td>

</tr>

<tr>

<td style="font-family:Helvetica,arial,sans-serif;font-size:16px;color:black;text-align:left;line-height:22px">

Dear ,

Your new eir bill is now available to view at my eir.

Your bill amount is € 44.44

Once you login to my eir, you can view and download a PDF of your bill, pay a bill and much more.

If you are set up for Direct Debit we will automatically take your payment. If not, you can set up Direct Debit at any time in my eir.

If you need help understanding your bill we have a full bill explanation available here.

```
<p> </p>

<p>Many thanks,</p>

<p>eir</p>

<p> </p>

<p style="font-size:11px">Please note this is an automated email.</p></td>

                                    </tr>
```

Impact

This allows a malicious actor on the same network as an Eir customer clicking on the link sent to them, or on the path between them and my.eir.ie, to take control of their interaction with my.eir.ie by either:

- sending them instead to a site impersonating my.eir.ie
- modifying the content returned by the initial HTTP GET request.

➢ *Vulnerability 2. Insecure login page*

It is standard practice to redirect the user to a secure https session first and only then serve the login page. This helps to secure the login process, and ensures the confidentiality of the login details entered by the user.

However, the http://my.eir.ie/login page immediately displays a dialog inviting the user to enter their email.

Doing so results in a HTTP POST to http://my.eir.ie/graphql/ containing a GraphQL query that contains the email address.


```
{"operationName":"getBrands","variables":{"emailAddress":"john.doe@gmail.com"},"que
ry":"query getBrands($emailAddress: String!) {\n  getBrands(emailAddress:
$emailAddress) {\n    brand {\n      system\n      mobileNumber\n      billType\n
      title\n  __typename\n      }\n    __typename\n  }\n}\n"}
```


Alternatively, the user may click a “forgotten your email” link. This also results in an HTTP POST, this time a GraphQL query containing the phone number.


```
{"operationName":"createNumberValidaion","variables":{"number":"027123456","recapt
cha":"03AKH6MRFAeHMWfsjb7UejNAHN1SZ41crDOhj1s49CsRTxb7pDnfsf4gSZqwGc2-
Wx9F1k017XTBqrug5lsP9Va__xQ-
vxatXfOtXWergckWEfinCdF6rV99eWveUifToSkY4o9J2HN8XoaleE9lWHVu77hsV6TJr44SJAx
YDLOD3ELJ9k8YUY3CZJsl7OgDVE_r8Ie_O6dea3WPK0prCJvS8eaWIjYLXhE2iokS2WMGzHPJ
MasmGFQQVZHaxK1Ikhz6OtPM-99R8BjrzAPyeA4N3Dg0Iv0UeJsQvKDYVmJE6nZZ4mbP-
LmkMS6UhQkOKwqp0H9GO9d3cSAHomZrAiMZjy11ZWr86h9qTyczytFukja4P0Nk7aru4_T-
QTVvKVuVPob1MrrhitqjQdUff3voxhfQNF6STcye5b6jjHV2BSygjPMkTkJEzudOYHdOtt2sSBR
KX5D7CwcSYUPL44W_iRU9vkx7t9_zSo4S9SQaFr0DQzHGxN6SEVZ1UFSWtFKy9wGAz0KKIX
xE37KTzIRa_G6LiGcj1-yQ6oj8iscEPZ-ff47F_Kx6Jf3v2l6Fm3MVsojY-
jQY4gsGO134QqWeY9mgBZ-oULTA"},"query":"mutation
createNumberValidaion($number: String!, $recaptcha: String!) {\n
createNumberValidation(number: $number, recaptcha: $recaptcha) {\n    otpUuid\n
      statusCode\n  mobileNumber\n      __typename\n  }\n}\n"}
```


Impact

Because the connection is still at this point unencrypted, all the above information is readable by anyone on an adjacent network.

➢ *Vulnerability 3. Unprotected GraphQL web service*

A principle of login page design is that it should reveal the least possible amount of information to a malicious actor attempting to login. Descriptive error messages are frowned upon, as “unknown user” versus “incorrect password” helps the would-be attacker. This principle is not followed here, as the email address is validated on its own first. But that is not the real problem.

The real problem is that the way this is done by the my.eir.ie page is to expose an unauthenticated worldwide accessible GraphQL web service endpoint that not only validates the user, but also reveals information about them when successful.

The email validation POST described above results, when successful, in a response that contains not just whether the email address is that of an Eir customer, but also the last 4 digits of their phone number and a “billType” field.

{"data":{"getBrands":{"brand":[{"system":"portal","mobileNumber":"***-***4567","billType":"Fixed_Bill","title":null,"__typename":"Brands"}],"__typename":"Brand"}}}

Impact

A malicious actor could retrieve information about known Eir customers from anywhere on the Internet.

Responsible Disclosure

In accordance with Corrata’s Responsible Disclosure, Eir was notified.
They have since indicated that those vulnerabilities have been resolved to their satisfaction.
