Business Logic Errors in crater-invoice/crater

0

Valid Reported on Jan 27th 2022

Description

It is found that comapny currency can not be changed since the field is disabled as shown in the screenshot but it can be changed by tampering the parameter.

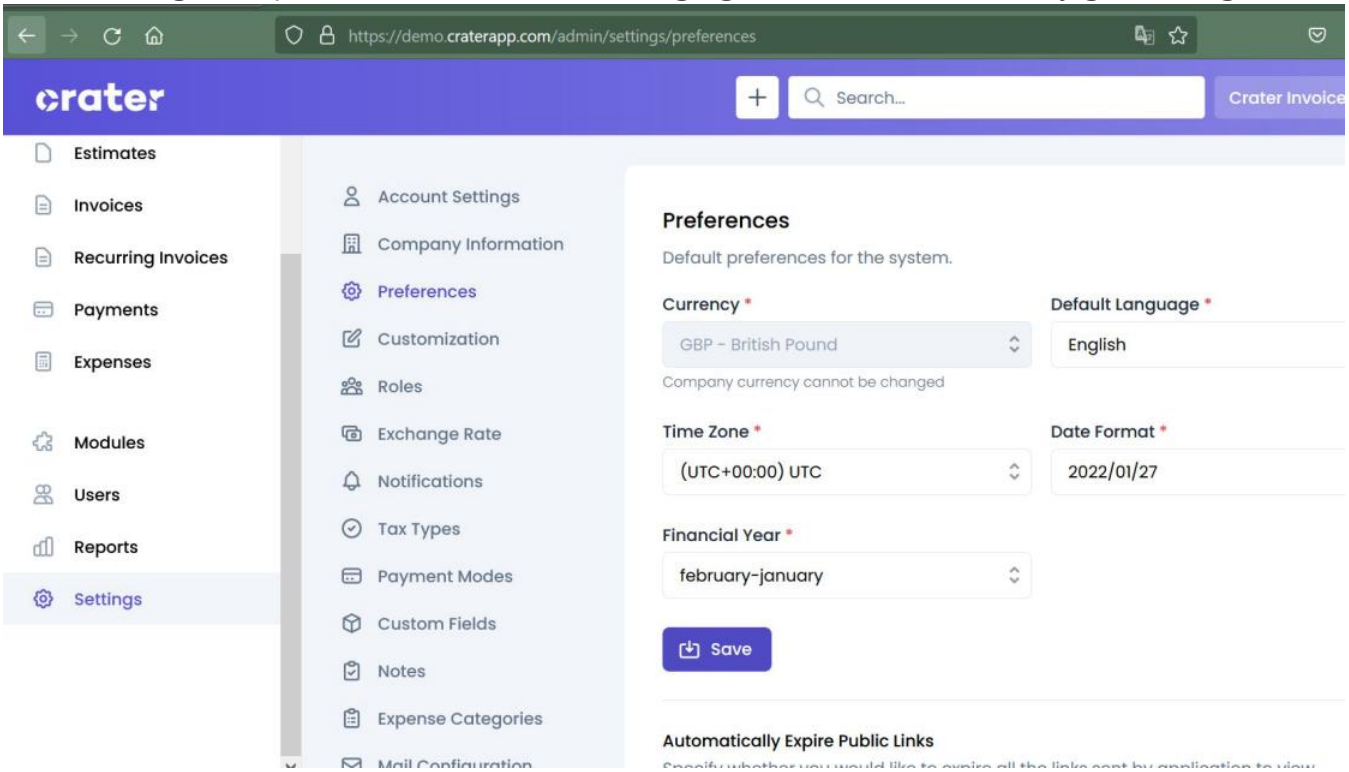
Proof of Concept

Actual Request

```
POST /api/v1/company/settings HTTP/1.1
Host: demo.craterapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
company: 1
Content-Type: application/json;charset=utf-8
X-XSRF-TOKEN:
Content-Length: 3344
Origin: https://demo.craterapp.com
Connection: close
Referer: https://demo.craterapp.com/admin/settings/preferences
Cookie:
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"settings":{"invoice_auto_generate":"YES","payment_auto_ge
```

In the above request you can see that currency value is set as 1 which is US dollar which can not be changed as per the screenshot. But changing the value to 2, currency gets changed.



Impact

Since different currency have different value, it might affect the company financially.

CVE
CVE-2022-0514
(Published)

Vulnerability Type
CWE-840: Business Logic Errors

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

shubh123-tri

@shubh123-tri

unranked

This report was seen 347 times.

We are processing your report and will contact the **crater-invoice/crater** team within 24 hours.
10 months ago

We have contacted a member of the **crater-invoice/crater** team and are waiting to hear back
10 months ago

Mohit Panjwani 10 months ago Maintainer

Hey, Thanks for the report but I don't think this is a major issue because only the owner of the company / super admin can access this endpoint.

shubh123-tri 10 months ago Researcher

But it has already been in a disabled state and should not be allowed to change in either case

We have sent a follow up to the **crater-invoice/crater** team. We will try again in 7 days.
10 months ago

We have sent a second follow up to the **crater-invoice/crater** team. We will try again in 10 days.
10 months ago

Mohit Panjwani validated this vulnerability 10 months ago

shubh123-tri has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **crater-invoice/crater** team. We will try again in 7 days.
10 months ago

We have sent a second fix follow up to the **crater-invoice/crater** team. We will try again in 10 days. 9 months ago

We have sent a third and final fix follow up to the **crater-invoice/crater** team. This report is now

considered stale. 9 months ago

Mohit Panjwani marked this as fixed in 6.0.5 with commit fadef0 8 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

Sign in to join this conversation