

Inefficient Regular Expression Complexity in chatwoot/chatwoot

0

Valid Reported on Jun 30th 2021

Description

If we want to use Regex in our match or search or replace or ... functions, we must be sanitize this function's inputs. if an attacker capable to inject any Regex or abuse the bad Regexes that used in our codes, then the ReDoS vulnerability appear and according to "freezing the web a study of redos vulnerabilities in javascript-based web servers" Paper if the web server be JavaScript-based and also be Nodejs, this probability exists that one user can do DoS attack that affect on response time of all users from server as Nodejs has a single-thread functionality.

Proof of Concept

```
// payload
a= "<style fdfasfafasdfasfasdfs</style> "
```

According to [1] Permalink the mentioned line is vulnarable to ReDoS and also the `stripStyleCharacters` method used in [2] Permalink and at the end the bad regex used in Conversion section of Chatwoot. I started send message from my Gmail to the created mail address of conversations section and I exponentially increase the lenght of payload like this: a, 2*a , 4*a , ... 200*a and measure the notification time on both my other email and conversation box and obviously it is take much more time in 200*a payload. you can test it with your own way.

Impact

This vulnerability is capable of Direct impact on Availably of whole system.

Occurrences

- JS EmailContentParser.js L2
- Message.vue L143

CVE

CVE-2021-3649

(Published)

Vulnerability Type

CWE-1333: Inefficient Regular Expression Complexity

Severity

High (7.5)

Affected Version

*


Visibility

Public

Status

Fixed

Found by



amammad

@amammad

pro

This report was seen 261 times.

- We have contacted a member of the chatwoot team and are waiting to hear back

a year ago
- amammad modified the report

a year ago
- Jamie Slome

a year ago

Admin
- Hey all, just a heads up that we adjusted the CWE to Inefficient Regular Expression Complexity on request from the disclosing researcher.
- amammad

a year ago

Researcher

Hi dear chatwoot's team
I just want to know that you receive this report and if I can help you more and more, just tell me now.
have a good developer days :)

Pranav Raj S validated this vulnerability a year ago

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Pranav Raj S marked this as fixed with commit aa7db9 a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

amammad a year ago

Researcher

Thank you so much, dear Pranav.
I encourage to find more bugs in your application.

Jamie Slome a year ago

Admin

Waiting to publish the CVE:

<https://github.com/CVEProject/cvelist/pull/2281>

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team