Chatwoot's Misconfigured Rack_Attack.rb Does Not Appropriately Protect Against Brute Force Attacks in chatwoot/chatwoot

2

✓ Valid Reported on Jun 10th 2022

Description

Chatwoot relies on the rack_attack.rb file to defend the application against various brute force attacks. The Chatwoot application fails to prevent brute force attacks against the listed paths when strings are appended to the end of POST directory names. Some protection still exists, primarily where more than 300 requests are made in a minute, which appears to be a default rule for the application and configuration. Provided an attacker keeps attacks within 300 per minute it is possible to bypass the configured rules.
The vulnerability was discovered in all tested directories, including:
-- /auth/sign_in.json
-- /api/v1/accounts.json
-- /super_admin/sign_in.json
As I cannot configure the environment to test the other parameters, I am unsure if they are vulnerable, however the directories do accept random strings appended to the end. NOTE - Any arbitrary add on to the end of the directory can bypass the restrictions.
Note that I have tested a possible fix for the issue locally by modifying existing rack_attack rules.

Proof of Concept

```
POST /auth/sign_in.json HTTP/1.1
Host: 192.168.1.3:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.3:3000/app/login
Content-Type: application/json
Content-Length: 74
```

```
Content-Length: 74
Origin: http://192.168.1.3:3000
DNT: 1
Connection: close
Cookie: _chatwoot_session=isHDBFZBkWRHKTcjNmQPFlXVrtaswMNx7FNWeWpiULOnK%2F

{"email":"joe@mayorsec.com","password":"Password123!","sso_auth_token":""}
```

```
POST /super_admin/sign_in.json HTTP/1.1
Host: 192.168.1.3:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100
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
Referer: http://192.168.1.3:3000/super_admin/sign_in
Content-Type: application/x-www-form-urlencoded
Content-Length: 234
Origin: http://192.168.1.3:3000
DNT: 1
Connection: close
Cookie: _chatwoot_session=1eo0NEleyD9vD3SZGSC5fmQ8%2FqjqauSZabHRTb79DXjlOr
Upgrade-Insecure-Requests: 1

authenticity_token=WWh5xWO3jgXwVKZb3zWM94qL52osMpbCpFFeuxRsdlgb%2B7OtMdtb%
```

```
POST /api/v1/accounts.json HTTP/1.1
Host: 192.168.1.3:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.3:3000/app/auth/signup
Content-Type: application/json
Content-Length: 144
Origin: http://192.168.1.3:3000
DNT: 1
Connection: close
```

```
Cookie: _chatwoot_session=pOArRsb8vDx6%2FpQuywQLE3E0lznJlbGrnqLLNMT9ySqt7YF

{"account_name":"KATHRINE","user_full_name":"KATHRINE","email":"KATHRINE@ma
```

Impact

Impact varies for each individual vulnerability in the application. For generation of accounts, it may be possible, depending on the amount of system resources available, to create a DoS event in the server. These accounts still need to be activated; however, it is possible to identify the output Status Code to separate accounts that are generated and waiting for email verification.
For the sign in directories, it is possible to brute force login attempts to either login portal, which could lead to account compromise.

Occurrences

rack_attack.rb L76
rack_attack.rb L62
rack_attack.rb L46
rack_attack.rb L57
rack_attack.rb L85
rack_attack.rb L67
rack_attack.rb L52

References

- CWE-307 Improper Restriction of Excessive Authentication Attempts
- OWASP OAT-019 Account Creation
- OWASP Top 10 - A2:2017 Broken Authentication

CVE
CVE-2022-3741
(Published)

Vulnerability Type
CWE-307: Improper Restriction of Excessive Authentication Attempts

Severity
Critical (9.4)

Registry
Other

Other

Affected Version
V2.5/V2.6

Visibility
Public

Status
Fixed

Found by

Joe Helle
@dievus
master

This report was seen 1,157 times.

Joe Helle 6 months ago Researcher

I would also request that this finding to receive CVE status IF accepted.

Joe Helle modified the report 6 months ago

Joe Helle 6 months ago Researcher

Image evidence available here - https://themayor.notion.site/Rack_Attack-rb-Issue-3adb70ea251649d69af0e7822a23f493

Joe Helle modified the report 6 months ago

Joe Helle modified the report 6 months ago

Joe Helle modified the report 6 months ago

Joe Helle submitted a patch 6 months ago

Joe Helle 6 months ago

Chat with us

Commit removed until I hear from the maintainer.

Joe Helle modified the report 6 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

We have contacted a member of the **chatwoot** team and are waiting to hear back 5 months ago

Joe Helle 5 months ago Researcher

Please note that I do have a locally confirmed fix for the issue once accepted.

Joe Helle modified the report 5 months ago

We have sent a follow up to the **chatwoot** team. We will try again in 7 days. 5 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

Joe Helle modified the report 5 months ago

We have sent a second follow up to the **chatwoot** team. We will try again in 10 days. 5 months ago

We have sent a third and final follow up to the **chatwoot** team. This report is now considered stale. 5 months ago

Sojan Jose modified the Severity from Critical to Low 5 months ago

Sojan Jose validated this vulnerability 5 months ago

Joe Helle has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Joe Helle 5 months ago Researcher

Hi @maintainer. What is the justification for the massive reduction in criticality? @admin this is one of those times that I brought up in a Issues post where the modification is not appropriate.

Joe Helle 5 months ago Researcher

https://www.cvedetails.com/cve/CVE-2022-29084/

https://www.cvedetails.com/cve/CVE-2021-41435/ - unrestricted log in attempts based on a programmatic error

https://www.cvedetails.com/cve/CVE-2018-5469/

Yes, there are scores that are also lower than these. But the issues with the application programmatically, and the amount of APIs that are vulnerable, we're factored into the score.

@admin I have pending disclosures on this platform for the same issue, and the maintainer agreed with the high rating as well. I mean no disrespect here, but the significant differences in severity rating is not only infuriating, it's boggling. There needs to be a way for industry professionals who do this every day to have some amount of say in this process. It's not just a score applied to get the most money I can.

Jamie Slome 5 months ago Admin

Just marking this as in discussion via LinkedIn 👍

We have sent a fix follow up to the **chatwoot** team. We will try again in 7 days. 5 months ago

Joe Helle 5 months ago Researcher

@admin Just FYI with another publicly disclosed Rack Attack vulnerability. Note that the maintainer was happy to discuss the score, and we settled on 8.2 with CVE to follow. Note that the Chatwoot finding here is more severe as Chatwoot's misconfiguration affects authentication, whereas the disclosure below affected password resets and other functions such as ticket submissions.

https://huntr.dev/bounties/d914fd3c-9c48-4d4e-a3b2-6b8d09b0f229/

Chat with us

Jamie Slome 5 months ago Admin

@Sojan - would be good to understand the reasoning around the reduction in severity, but also, do you have any qualified thoughts on the new references provided by @dievus?

Joe Helle 5 months ago Researcher

https://huntr.dev/bounties/3055b3f5-6b80-4d47-8e00-3500dfb458bc/

Joe Helle 5 months ago Researcher

^ Just an authentication endpoint as opposed to two authentication endpoints and other APIs as is the issue here.

We have sent a second fix follow up to the **chatwoot** team. We will try again in 10 days. 4 months ago

We have sent a third and final fix follow up to the **chatwoot** team. This report is now considered stale. 4 months ago

Sojan Jose 3 months ago Maintainer

@joe @jamie, I missed out on the conversations over this thread. As per the security policy of chatwoot https://github.com/chatwoot/chatwoot/blob/develop/SECURITY.md we don't consider DOS attacks into the vulnerability program. But we wanted to appreciate the effort put forward into this report.

The system is also configured with 300 requests per minute limit, so the team didn't feel this was a critical vulnerability.

Joe Helle 3 months ago Researcher

The issue isn't denials of service. No appropriate security policy anywhere would allow 300 login attempts per minute, in an environment where an attacker can otherwise bypass your hard coded rules, which is the case here.

You'll have to forgive me for feeling like this being the exact definition of a bug hunter finding a 100% valid bug in your code that has real world implications, backed up by other reports with the exact same issue, at a far higher criticality.

Joe Helle 3 months ago Researcher

@admin so what do we do here?

Joe Helle 3 months ago Researcher

Sorry the last message cut off.

The finding has nothing to do with denial of service.

I have other valid reports on this platform with less impact and higher criticality that have been validated and agreed upon by developers/maintainers

Joe Helle 3 months ago Researcher

You guys literally just disclosed a High finding with account brute force and rated it at a High. https://huntr.dev/bounties/6-chatwoot/chatwoot/, which was for a completely different issue evidently.

And I can tell you right now that your rack attack fix for that report likely doesn't fix the issue found in mine.

Sojan Jose 3 months ago Maintainer

@Joe Helle Internally, when we receive security reports, we classify the priority based on how quickly we have to address it. (create a hotfix, fix it in the next release, and keep it in the backlog for a future release) etc. While validating the report, we updated the severity to reflect our internal tracking; there was no other ill intent. The ability for the maintainers to update the severity was introduced by huntr only a few months back. (hence the disparity between the report /6-chatwoot/chatwoot/)

The team reviewed this report and realized we could have handled this instance better. Therefore, we will revert the severity to high. We want to reiterate our appreciation for your efforts and apologize for the frustration caused.

To enhance transparency, We will update our security report guidelines with more details about the internal process and discuss the severity with the reporter in instances where we decide to update it.

Chat with us

Sojan Jose 3 months ago Maintainer

@Jamie Slome, I can't find an option to bump up the severity. Could you please help us with that?

Joe Helle 3 months ago Researcher

Thank you for that @sojan. I appreciate your transparency and working with me on the issue.

In the meantime, your updated Rack Attack file is vulnerable to the attack outlined in this report. The issue is that you are using absolute directory paths (i.e. req.path ==). I just pulled this from the 2.8.1 hotfix.

```
throttle('accounts/ip', limit: 5, period: 5.minutes) do |req|
  req.ip if req.path == '/api/v1/accounts' && req.post?
 end
```

This would be better suited to use req.path.starts.with?(<directory path>). I'm not a Ruby developer so I don't know exactly why, but the engine is processing the path with the characters appended to the end. Since the Rack config uses absolute paths, the engine isn't recognizing it as a protected API call.

I worked a similar vulnerability with an organization using a similar configuration. You can see how they implemented a working fix here - https://github.com/zammad/zammad/blob/e30aefa465ad395dd68677d0599ea3da53df4a5b/config/initializers/rack_attack.rb#L14.

I will submit my recommended fix through the dashboard here for your review. Thank you Sojan.

Joe Helle submitted a patch 3 months ago

Jamie Slome 3 months ago Admin

Happy to update the severity to `High` 👍

@Sojan - can you please provide the CVSS vector you would like me to use?

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Chat with us

Joe Helle 3 months ago

Any update here @sojan ?

Sojan Jose 2 months ago Maintainer

@jaime @joe let me know if the vector looks good

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Sojan Jose 2 months ago Maintainer

We have added a fix for the same in https://github.com/chatwoot/chatwoot/commit/9525d4f0346a2fdac13a0253f9180d20104a72d3

which will be available with our upcoming release.

Joe Helle 2 months ago Researcher

Awesome. I’ll look at it soon. @admin when you correct the score can you also please refund me the point that was taken? And will the score correction appropriately set the bounty amount?

Thanks!

Joe Helle 2 months ago Researcher

Will also need CVE assigned

Joe Helle 2 months ago Researcher

@sojan I agree with the CVSS.

Have you tested the fix with the way I've been exploiting it? My biggest concern would be the use of regular expression that it looks like you've defined here as I didn't do much testing beyond the ".extension" add-ons I was using. Regex has a way of being bypassed, so I would definitely want to make sure you've tried a variety of injections at the end, especially characters like %.

Joe Helle 2 months ago

Chat with us

I did just test with the change and it appears to work, but again, using regex can open up new

I did just test with the change and it appears to work, but again, using regex can open up new challenges. But from my perspective and a few minutes of testing it appears to be functioning as you would expect.

Jamie Slome 2 months ago Admin

Hey all, happy we have found a pathway forward here :)

Firstly, the CVSS vector provided @sojan results in a critical score (`AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L`) of 9.4. If you are happy with this, I will proceed to update the severity. We will also make sure to bump the bounty back to the relevant severity bracket.

Regarding the CVE, @sojan, are you happy for a CVE to be published for this report?

Jamie Slome 2 months ago Admin

I am following up on the above, as you previously mentioned that the severity should be increased to `High` . Just double checking whether it should be `High` or `Critical` , given the CVSS vector string you provided results in `Critical` .

Joe Helle 2 months ago Researcher

Hi there @maintainer @admin. Just wanted to follow up on this as several weeks have passed since the last updates.

Joe Helle a month ago Researcher

@sojan any update?

Joe Helle a month ago Researcher

@jamie @admin they have patched and made the fix live for this as far as I can find. As this is a managed Huntr project can you please help mediate here. The rating should have been increased, and as such this should be eligible for a bounty payout.

Additionally, can I get the point back that was initially removed with the incorrect CVSS assessment on their end?

Thank you.

https://github.com/chatwoot/chatwoot/blob/develop/config/initializers/rack_attack.rb

Chat with us

Joe Helle a month ago Researcher

Here's the commit - https://github.com/chatwoot/chatwoot/commit/9525d4f0346a2fdac13a0253f9180d20104a72d3

Sojan Jose a month ago Maintainer

@jamie Please go ahead.
@joe, sorry for missing out on the notifications on this.

Sojan Jose marked this as fixed in v2.10.0 with commit 9525d4 a month ago

The fix bounty has been dropped ✗

This vulnerability has been assigned a CVE ✓

rack_attack.rb#L52 has been validated ✓

rack_attack.rb#L57 has been validated ✓

rack_attack.rb#L85 has been validated ✓

rack_attack.rb#L46 has been validated ✓

rack_attack.rb#L76 has been validated ✓

rack_attack.rb#L67 has been validated ✓

rack_attack.rb#L62 has been validated ✓

Joe Helle a month ago Researcher

Thank you @sojan

@admin can we please get the CVE ID and scoring updated please? I'd love to finally get this one paid out and behind us. Thank you.

Chat with us

Pavlos a month ago Admin

Hey Joe! As soon as Sojan publishes this report a CVE will be assigned :)

Joe Helle a month ago Researcher

@pavlos was the score going to be changed too? Everything still shows low.

Joe Helle a month ago Researcher

@admin @pavlos it's now been posted and there is no severity increase nor bounty payment. Can we please remedy this?

Joe Helle a month ago Researcher

@jaime @joe let me know if the vector looks good

Per @sojan,

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Per @jamie
Hey all, happy we have found a pathway forward here :)

Firstly, the CVSS vector provided @sojan results in a critical score (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L) of 9.4. If you are happy with this, I will proceed to update the severity. We will also make sure to bump the bounty back to the relevant severity bracket.

Regarding the CVE, @sojan, are you happy for a CVE to be published for this report?

Sojan Jose published this vulnerability a month ago

Ben Harvie a month ago Admin

This report has now been remedied as requested, happy hunting:)

Sign in to join this conversation

Chat with us