Allocation of Resources Without Limits or Throttling in koel/koel

0

Valid Reported on May 20th 2021

✍️ Description

Koel is lacking any form of rate limiting in the login form, thus allowing an attacker to brute force their way in.

🦹 Proof of Concept

Spin up an instance of Koel.
Open up burpsuite and capture a login request, send it to intruder, set your options and run.
401 is shown when invalid, 200 is shown when valid.

💥 Impact

This can lead to full account takeover, including admin accounts which have dangerous permissions.

💡 Mitigation

Implement max login attempts
Implement a password strength policy

Vulnerability Type
CWE-770: Allocation of Resources Without Limits or Throttling

Severity
High (7.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Cyberlytical
@cyberlytical
unranked

Fixed by

Phan An
@phanan
maintainer

This report was seen 424 times.

Cyberlytical 2 years ago — Researcher

First timer here, excuse any mistakes in submitting

Jamie Slome 2 years ago — Admin

All looking good!

Phan An 2 years ago — Maintainer

Koel's developer here. I can't reproduce the vulnerability. You can see here that a `throttle` middleware is in place, and my test just now shows that it works with this reponse payload after a certain number of login requests:

```
exception: "Illuminate\\Http\\Exceptions\\ThrottleRequestsException"
file: "/local/koel/koel/vendor/laravel/framework/src/Illuminate/Routing/Middleware/Thr
line: 200
message: "Too Many Attempts."
```

Phan An 2 years ago Maintainer

Since the "here" link in my previous comment doesn't have a very recognizable styling, here is the URL: https://github.com/koel/koel/blob/master/app/Http/Kernel.php#L57

Cyberlytical 2 years ago Researcher

Hey there, that's weird. How many attempts does it allow? Intruder had gotten well over 500 attempts before it got a weak password.
If the throttling is unable to reproduce, then no password policy is still an issue worth resolving

Phan An 2 years ago Maintainer

Hmm. I guess the problem here is Laravel (the framework powering Koel) calculates a request's signature using the domain and the request IP:

```
if ($user = $request->user()) {
    return sha1($user->getAuthIdentifier());
} elseif ($route = $request->route()) {
    return sha1($route->getDomain().'|'.$request->ip());
}
```

So if a tool can somehow fake these values, it can fool the limiter. The good news is , Laravel (or rather, one of its first-party packages) has another Trait specifically for login throttling called `ThrottlesLogin` with uses the username field and the IP address for the signature:

```
protected function throttleKey(Request $request)
{
    return Str::lower($request->input($this->username())).'|'.$request->ip();
}
```

So I'll use this trait as the fix. Thank @Cyberlytical a lot for the report!

Cyberlytical 2 years ago Researcher

Perfect, thank you!

Sign in to join this conversation