

Vulnerability Vector: <https://sisudata.com/blog>

Vulnerability: Spam & SMTP denial of service vector due to lack of rate limiting & email confirmation on newsletter sign up

Severity: None⇒Low

Vulnerability Description:

Lack of email confirmation or validation when signing up for a newsletter or service that involves receiving a constant stream of emails can lead to spamming vectors, and potential backend database/SMTP denial of service potential.

Vulnerability Impact:

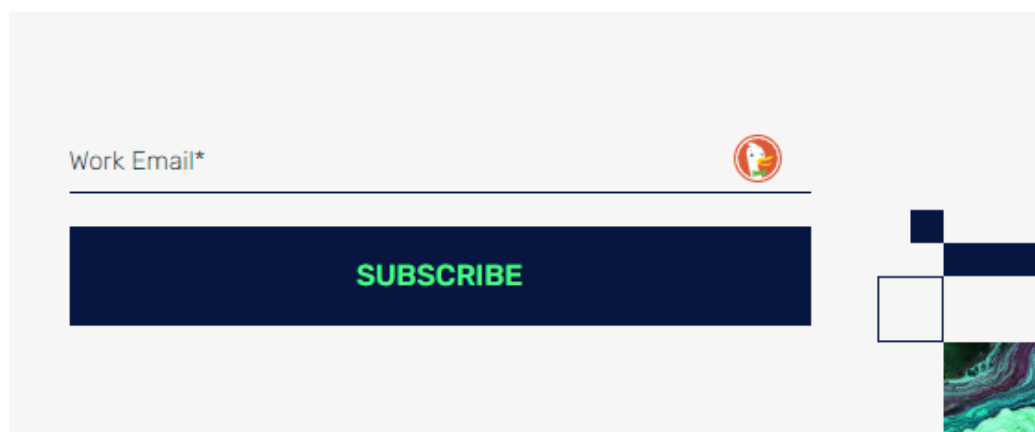
A bad actor, or someone who is looking to cause destruction or abuse to the websites services, can take advantage of the lack of confirmation when signing up to the newsletter service, they can:

- maliciously sign email addresses/users up without their consent or confirmation, flooding their inbox with unwanted emails and letters
- send false or high amounts of email addresses up to the service, potentially causing a slowdown or complete denial of service when legitimate emails are being sent out to users as part of the newsletter.

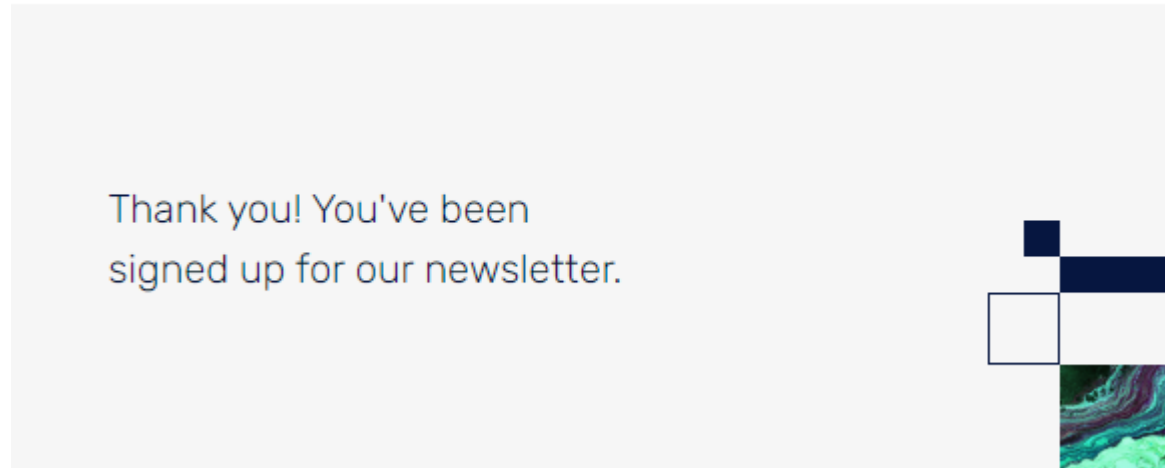
If a threat actor is able to successfully exploit this issue, they may be able to flood a victims inbox with unwanted spam and messages, and or have the email service used for the sending of newsletter emails blacklisted or reported as spam, leading the emails to potentially be listed as spam in the users mailbox, or not being sent to the user at all due to this.

Vulnerability findings:

When signing up to the newsletter service listed on the website:



No confirmation is asked to the user, or email sent to the inbox of the user asking for validation when signing up to the newsletter:



Vulnerability Exploitation/POC:

To further validate, and test the lack of rate limiting and confirmation on the newsletter sign up, captured the request being sent to the sign up page from the url listed in the **Vulnerability Vector** and reproduced the request from a different originating email addresses, effectively signing them all up to the newsletter:

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparatorLoggerExtensionsLearn

1 x2 x+

SendCancel<>>

Target: http

Request

PrettyRawHex

```
1 POST /index.php/leadCapture/save2 HTTP/2
2 Host: info.sisudata.com
3 Cookie: biz_uid=5de3b1c4afa846a4eabaaf8179eb7f72; _gcl_au=1.1.2049674753.1680278408; _ga=
GA1.2.168552301.1680278408; _gid=GA1.2.262783187.1680278408; _mktk_trk=
id:950-VPR-200&token: mch-sisudata.com-1680278408905-41326; cb_user_id=null; cb_group_id=null;
cb_anonymous_id=22f43b48fa-2e50-4672-9d86-29291776d973422; OptanonAlertBoxClosed=
2023-03-31T16:00:46.532Z; biz_flagsA=
47B422Version4223A142C422XDomain4223A422142242C422ViewThrough4223A422142242C422Fr4223A422142242C422
_biz_uid=3ae88; OptanonConsent=
18Gp:Enabled=0;datestamp=Fri;Mar+31+2023+19:31:4493A40+GMT+2B0100+(British+Summer+Time) &version=6.37.04
1s1AB61oba1=false;ghosts=1;landingPath=NotLandingPage(groups=C000343A03CC00043A03CC000243A03CC000143
Algeolocation=ML43B&AwaitingReconsent=false; gat_UA-12398733-1=1; _cf_bm=
bq4SbJdAgvWioFCq8IoKMFCCvN7R5J4Y.4FrAt4RRw-1680288588-0-AbcPQ8d871A6Axlbn8S8wt2IV7SH9uMy1JN2W161Lhb
8hBmPeV7khFNOCG9x0yKtmFqULGmv5Pz5tcbpmSaQ=; BIGipServers330web-nginx-app_https=
'AoGfaXwRzrMURunM2R0f1EEG2tC1kkqSdiXvpLck6rYaeBO6PyXa869b1fOK3JYHMsMsd5G7knfLE=; _biz_nA=31;
_biz_pendingA=
45B422m2Ffrm43Ffrm_c43D196352733426eMail43Dgoofysec42540proton.me426eventSource43DonSubmit426rnd43D6c
b66bbf818644baa5435ebc8cb17afa26_biz_u43D5de3b1c4afa846a4eabaaf8179eb7f72426_biz_s43D3ae88426_biz_l4
3Dhrcpt4253A4252F4252Fsisudata.com4252Fb1og426_biz_t43D1680288606378426_biz_i43DData4252C42520Analytic
s4252C42520And42520Machine42520Learning42520Blog42520V257C42520Sisu42520Data426_biz_m43D30422425D
4 Content-Length: 454
5 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
6 Accept: application/json, text/javascript, */*; q=0.01
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/111.0.5563.111 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://info.sisudata.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://info.sisudata.com/index.php/form/XDFrame
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19
20 Email=goofysec440proton.me&formid=1161&munchkinid=950-VPR-200&clearbitFormStatus=
Clearbit.Enrichment.Complete&2CCCompany&Company=Proton4 mkt_trk=
id43A950-VPR-200426token43A_mch-sisudata.com-1680278408905-41326&formid=1161&mktkReferrer=
https43A42F42Fsisudata.com42Fb1og426_biz_m43D3ae88426_biz_l43Dhrcpt4253A4252F4252Fsisudata.com4252Fb1og426_biz_t43D1680288606378426_biz_i43DData4252C42520Analytic
s4252C42520And42520Machine42520Learning42520Blog42520V257C42520Sisu42520Data426_biz_m43D30422425D
Email42Cformid42Cmunchkinid42Cc4learbitFormStatus42CCCompany42C_mkt_trk42Cformid42C_mktkReferrer4
checksum=3b9eb3fda44e57d126c2de9b61c129fa6c206da612431e5a7e0810cfc6077
```

Response

PrettyRawHexRender

```
1 HTTP/2 200 OK
2 Date: Fri, 31 Mar 2023 19:55:08 GMT
3 Content-Type: application/json; charset=utf-8
4 Cf-Ray: 7b0ace077faab7e2-AMS
5 Cf-Cache-Status: DYNAMIC
6 X-Form-Service-Request-Id: c7a2#18739060129
7 X-Marketo-Source: Form Service
8 Vary: Accept-Encoding
9 Server: cloudflare
10
11
12
13
14 {
  "formId": "1161",
  "followUpUrl": null,
  "allId": "eyJpIjo1THN1ZUJjZkRzVXprWUFBYyIsInQ1O1JkU05qVjZTYm5tZjZlOUVwQzpxemlBPT01fQ43D43D"
}
```

Resolution

The company receiving this report decided not to mitigate or take further action relating to this issue, but did note that potentially practises on forms like this would be rate limited in future, depending on severity and need.