Advisory ID: usd-2020-0054
CVE Number: CVE-2020-24710
Affected Product: Gophish
Affected Version: v0.10.1
Vulnerability Type: Stored Cross-Site S
Security Risk: Medium
Vendor URL: https://getgophish.com/
Vendor Status: Fixed

Description

Several occurrences of server-side request forgery were found during the pentest. These could be used to perform port scans of the server that hosts Gophish. In the majority of cases the error message resulting from querying the local server, with localhost or a loopback address, discloses the banner of the tested service. And in one case, where the banner was not visible, long response times indicated that the port was available. The screenshot below illustrates a successful port scan of the local host.

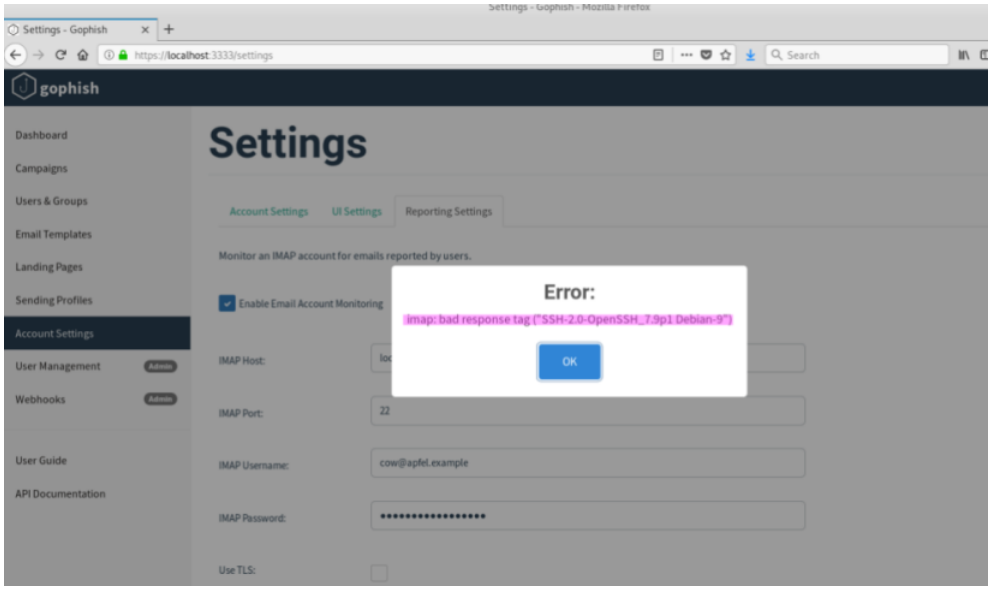
Proof of Concept (PoC)

URL: `/webhooks`
Comment: It is possible for a remote user to scan the open ports of the server that hosts the gophish admin application. Furthermore, the error messages reveals parts of the available service's banners. For example SSH's "Debian-9".

URL: `/sending_profiles`
Comment: It is possible for a remote user to scan the open ports of the server that hosts the gophish admin application. Open ports are disclosed by long response times after pressing the "Send" button of the "Send Test Email" feature.

URL: `/landing_pages`
Comment: It is possible for a remote user to scan the open ports of the server that hosts the gophish admin application. Furthermore, the error messages reveals parts of the available service's banners. For example SSH's "Debian-9".

URL: `/settings`
Comment: It is possible for a remote user to scan the open ports of the server that hosts the gophish admin application. Furthermore, the error messages reveals parts of the available service's banners. For example SSH's "SSH-2.0-OpenSSH_7.9p1 Debian-9".



Fix

A whitelist approach is not a valid solution when a user can make the application send requests to any external IP address or domain name. Despite knowing that the blacklist approach is not an impenetrable wall, it is the best solution in this scenario since it would inform the application to not send any requests to the server's loopback addr

Timeline

- 2020-06-18 First contact request via
- 2020-06-22 Vendor responds to initi
- 2020-08-20 Vendor publishes a fix h d3878347b005
- 2020-09-29 Security advisory releas

Credits

This security vulnerability was found b

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this security advisory is provided „as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.