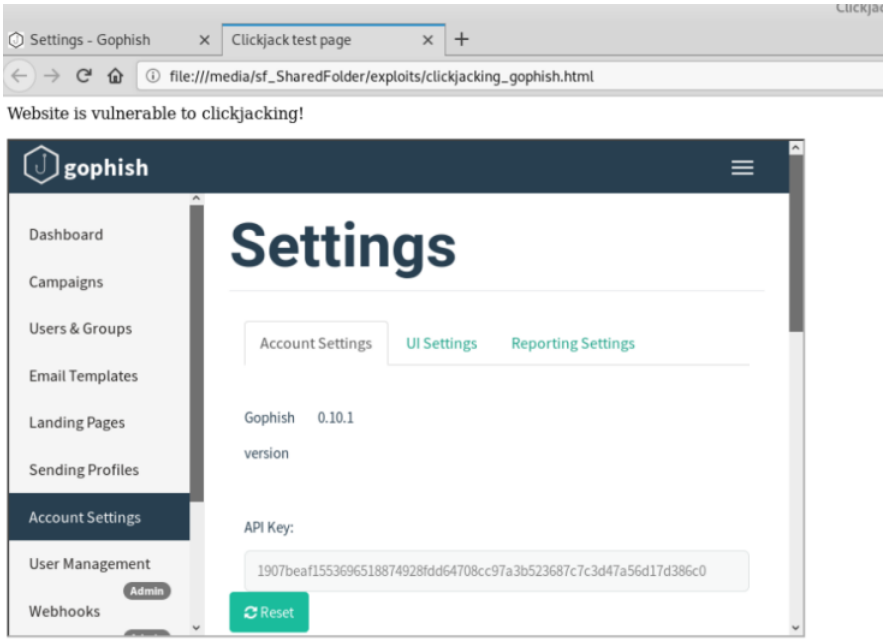
usd-2020-0051

Advisory ID: usd-2020-0051
CVE Number: CVE-2020-24711
Affected Product: Gophish
Affected Version: v0.10.1
Vulnerability Type: Improper Restricti
Security Risk: Medium
Vendor URL: https://getgophish.com/
Vendor Status: Fixed

Description

Gophish is vulnerable to clickjacking attacks. As can be seen in the screenshot below, it is the Reset button on the Account Settings page that is affected by this vulnerability. Since the Reset button resets the API key of the phishing framework, this vulnerability could enable and attacker to cause denial-of-service for services that are dependent on Gophish's API.

Proof of Concept (PoC)



Fix

It is recommended to use the frame-ancestors directive of the Content-Security-Policy header to prohibit a browser from rendering the content of the page inside an iframe. Alternatively, the same can be achieved by using the X-Frame-Options header. In both cases, the response header has to be set on every page to guarantee a proper protection against the attack. The exclusive use of framekiller JavaScript is discouraged. Detailed information on protection against clickjacking attacks can be found at OWASP: Clickjacking Defense Cheat Sheet.

Timeline

- 2020-06-18 First contact request via security@getgophish.com
- 2020-06-22 Vendor responds to initial contact
- 2020-08-07 Vendor publishes a fix
- 2020-09-29 Security advisory released

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.