



Alle akzeptieren

usd-2020-0051

Advisory ID: usd-2020-0051

CVE Number: CVE-2020-24711

Affected Product: Gophish

Affected Version: v0.10.1

Vulnerability Type: Improper Restriction of...

Security Risk: Medium

Vendor URL: <https://getgophish.com/>

Vendor Status: Fixed

Speichern

Nur technisch notwendige Cookies akzeptieren

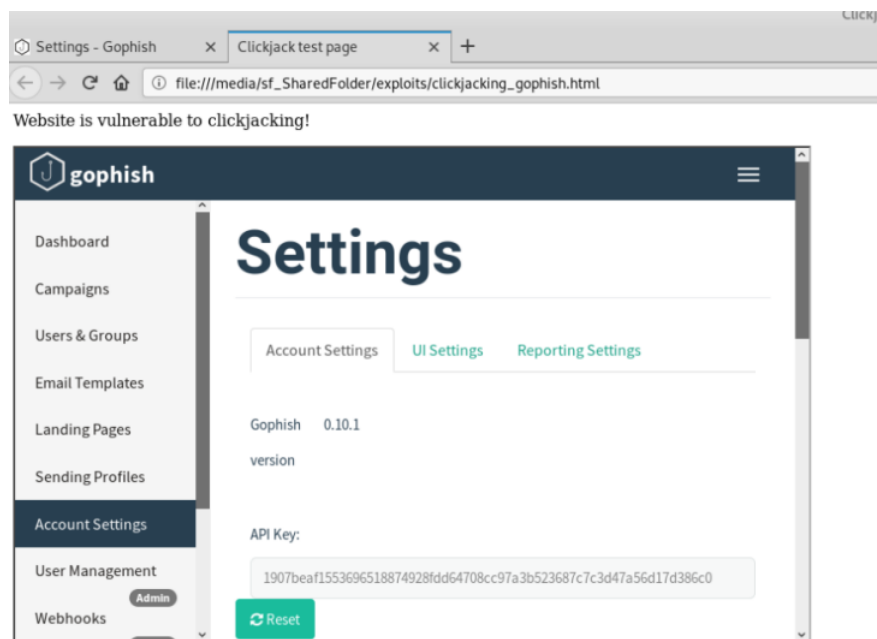
Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

## 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 an 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](mailto: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 by



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse Zwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



usd HeroLab

☒ Technisch erforderlich

☐ Analyse und Performance

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)



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.

[usd AG](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

[© 2022 usd AG](#)

[Meldung einer Schwachstelle oder eines Bugs](#)

[Code of Ethics](#)



[LabNews](#)

[Security Advisory zu GitLab](#)

[Dez 15, 2022](#)

[Security Advisory zu Acronis Cyber Protect](#)

[Nov 9, 2022](#)

[Security Advisories zu Apache Tomcat](#)

[Nov 24, 2022](#)