Advisory ID: usd-2020-0053
CVE Number: CVE-2020-24713
Affected Product: Gophish
Affected Version: v0.10.1
Vulnerability Type: Insufficient Sessio
Security Risk: High
Vendor URL: https://getgophish.com/
Vendor Status: Fix scheduled

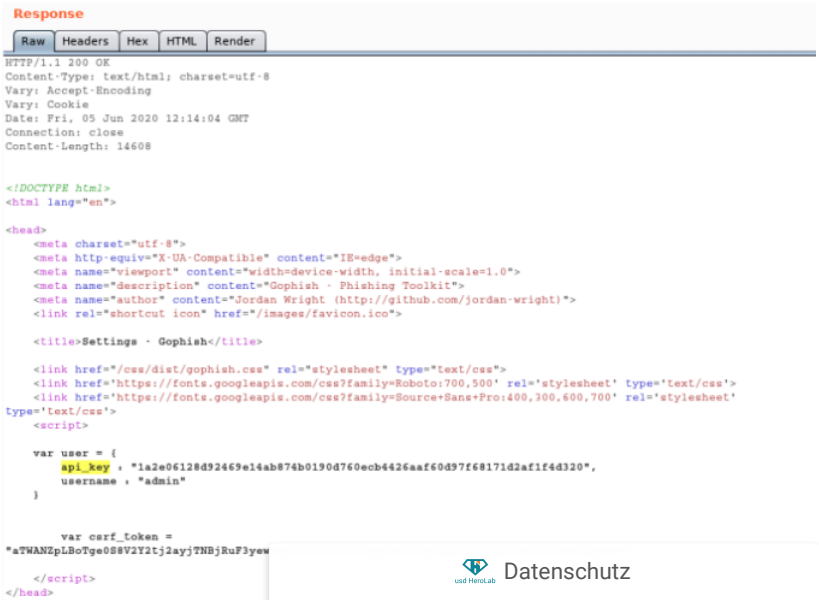
Description

The client's session cookie "gophish" doesn't get invalidated on the server side upon logout. A new cookie is sent to the client however the old session cookie can be used for browsing the settings page and to retrieve the API key.

Proof of Concept (PoC)

A user's session is not invalidated on the server-side upon logout. Hence, it is possible to continue browsing pages using the old session and a web application proxy such as Burp. The following screenshot illustrates how an HTTP request containing a logged out session returns the same response as if the session's owner was still logged in.

1. Logout using /logout
2. Replay previously captured request to `/settings` (including old cookie) – observe that the session was not invalidated server-side



Fix

Upon logout, user sessions should be

Timeline

- 2020-06-18 First contact request via
- 2020-06-22 Vendor responds to initi
- 2020-08-20 Vendor accepts the risk sue

About usd Security Advisories

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.