Advisory ID: usd-2020-0052
CVE Number: CVE-2020-24707
Affected Product: Gophish
Affected Version: v0.10.1
Vulnerability Type: CSV Injection
Security Risk: Medium
Vendor URL: https://getgophish.com/
Vendor Status: Fixed

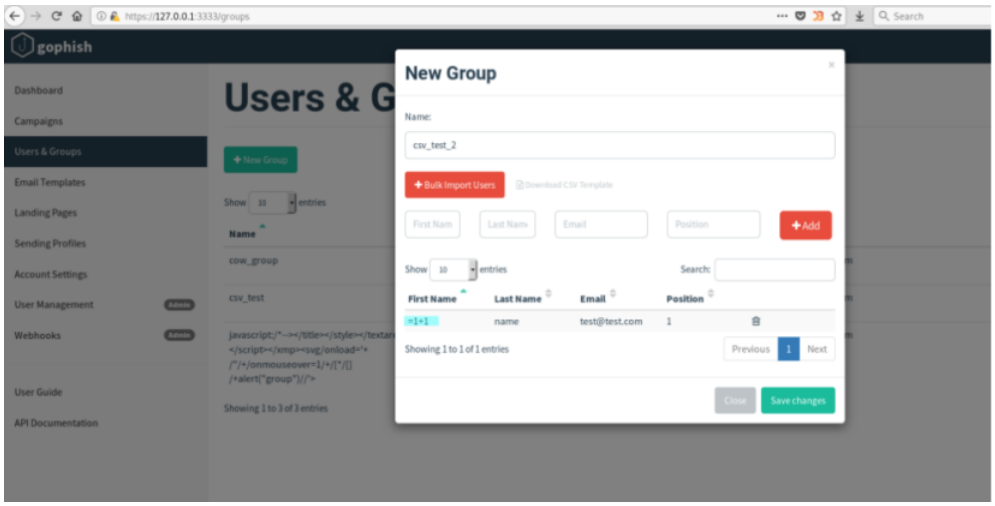
Description

Gophish allows the creation of CSV sheets which contain malicious content.

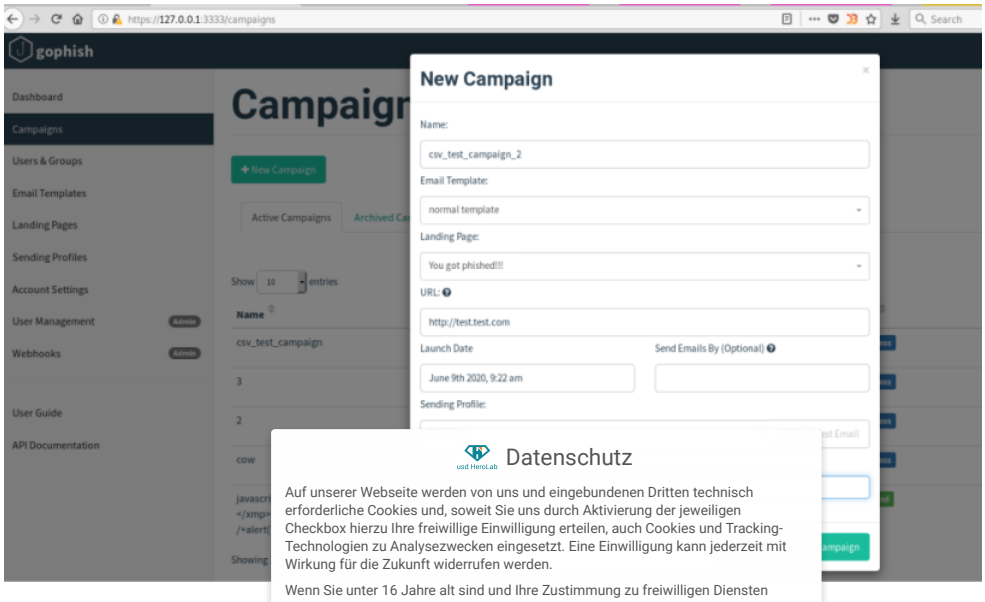
Proof of Concept (PoC)

The following screenshots show how a spreadsheet formula that is injected as the first name of a mail recipient executes when opened in a spreadsheet software such as Libreoffice Calc.

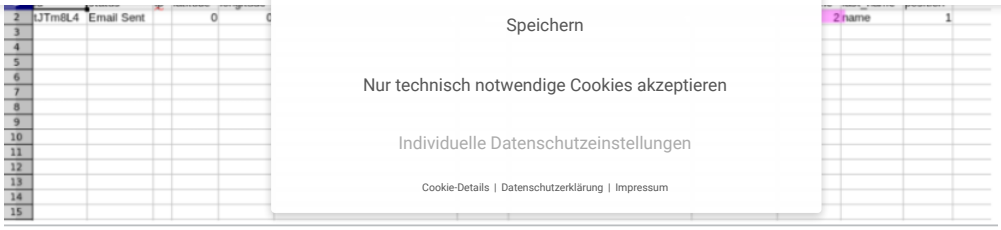
Inject Spreadsheet formular `(=1+1)` at `/groups`



Launch a campaign at `/campaigns`



Export campaign results as CSV and o



Most spreadsheet software supports the functionality of formulas as for example OpenOffice Calc or Microsoft Office Excel. Here, any cell starting with an equal- (=), a plus- (+) or a minus-sign (-) will be interpreted as a formula and may contain malicious code as shown in the example above. Additionally, older software versions interpret cells starting with an at-sign (@) as formulas as well.

For OpenOffice, this vulnerability is classified as CVE-2014-3524 which emphasizes the risk of unfiltered spreadsheets. Due to this vulnerability, an attacker can take over the control of a victim's system or gain unauthorized access to private resources.

Fix

It is recommended to restrict the set of allowed characters as much as possible for all user input. This can, for example, be realized with a whitelist. Additionally, every cell that starts with an equal- (=), a plus- (+), a minus- (-) or an at-sign (@), or contains a comma (,) or a semicolon (;) should be embedded in double quotes („) when generating spreadsheets, such as csv, xls or xlsx files, automatically. Furthermore, every double quote occurring within the content of a cell should be preceded by another double quote to avoid an early termination of the quoted string. In order to achieve this, a suitable library can be used.

Timeline

- 2020-06-18 First contact request via security@getgophish.com
- 2020-06-22 Vendor responds to initial contact
- 2020-07-25 Vendor publishes a fix https://github.com/gophish/gophish/commit/b25f5ac5e468f6730e377f43c7995e18f8fccc2b
- 2020-09-29 Security advisory released

Credits

This security vulnerability was found by Marcus Nilsson of usd AG.

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

Disclaimer

The information provided in this securi ecurity advisory may be updated in order to provide as accurate informati

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