



usd HeroL



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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



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 Analysezwecken 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 [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

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

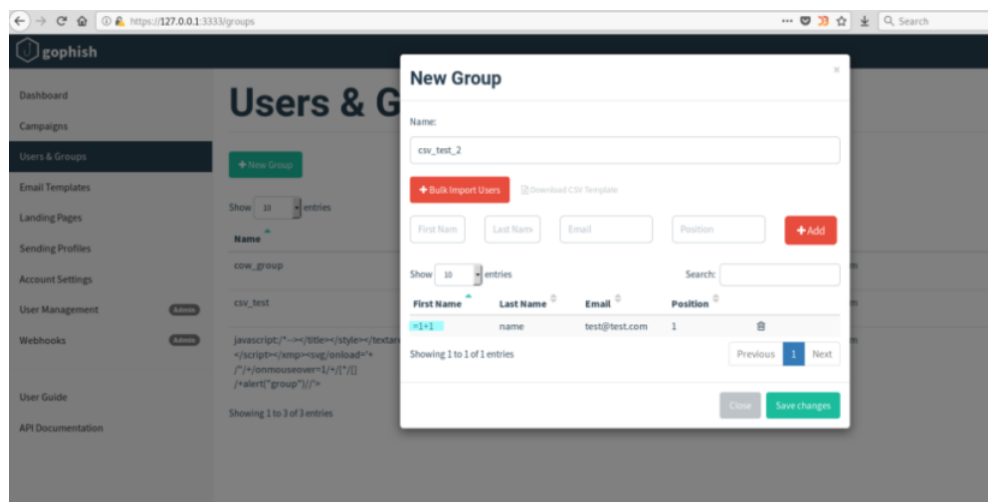
Description

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

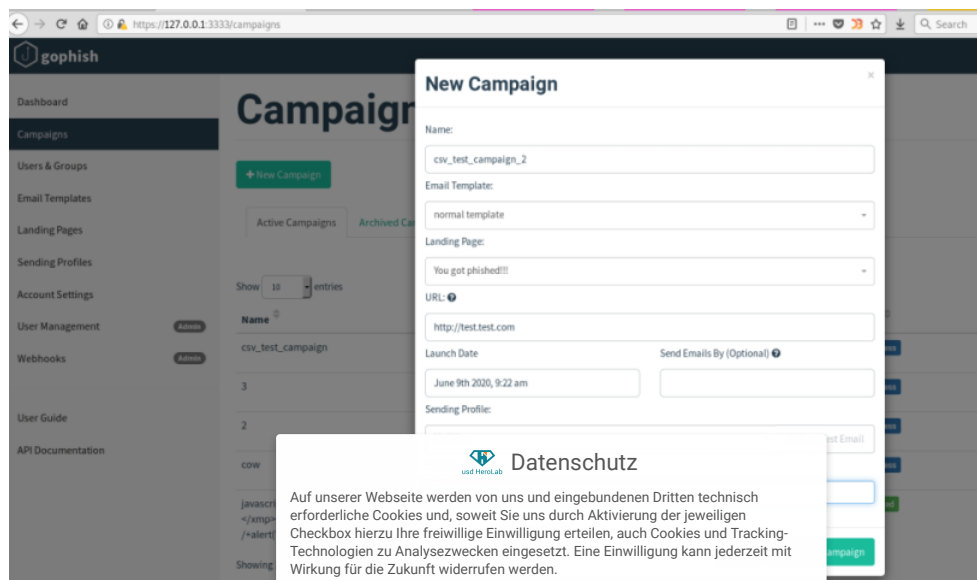
Proof of Concept (PoC)

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

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](#) | [Datenschutzerklärung](#) | [Impressum](#)

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/b25f5ac5e468f6730e377f43c7995e18f8fcc2b>
- 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



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technische erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse- und Marketingzwecken 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.



Disclaimer

The information provided in this security advisory may be updated in order to provide as accurate information as possible.

The information provided in this security advisory may be updated in order to provide as accurate information as possible.

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

[HeroLabs](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

© 2022 HeroLabs 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