



Alle akzeptieren

usd-2020-0029

**Advisory ID:** usd-2020-0029**CVE Number:** CVE-2020-27974**Affected Product:** NeoPost Mail Account**Affected Version:** 5.0.6**Vulnerability Type:** Reflected XSS**Security Risk:** High**Vendor URL:** <https://www.neopost.de/>**Vendor Status:** Not fixed

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

ware Pro 5.0.6

## Description

Reflected XSS attack (or non-persistent attack) occurs when a malicious script is reflected off of a web application to the victims browser. The attack is typically delivered via email or a web site and activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts.

## Proof of Concept (PoC)

The XSS attack was possible via the following url: `http://localhost/php/Commun/FUS_SCM_BlockStart.php?`

`code=%3Cscript%3Ealert(%27XSS%27)%3C/script%3E`

## Fix

Make sure to encode and/or filter the user supplied input.

## Timeline

- 020-03-25 This vulnerability was found during a Penetration Test on one of our customers
- 2020-03-26 First attempt to contact vendor
- 2020-05-14 Second attempt to contact vendor
- 2020-08-06 Third attempt to contact vendor
- 2020-09-23 Vendor was informed of upcoming release
- 2020-10-27 Security Advisory released

## Credits

This security vulnerability was found by Tim Kranz and Lars Neumann 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 dedicated to promoting security research through training courses and publications.

Always for the sake of our mission: „more security“

to usd AG



## 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.

in our practical work and our research to address current vulnerabilities and current security issues.



HeroLabs

☒ Technisch erforderlich

☐ Analyse und Performance

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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



## 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.

[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