usd-2020-0029 ware Pro 5.0.6

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

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 HeroLa n our practical work and our research through training courses and publicati abilities and current security issues.

Always for the sake of our mission: „m

to usd AG

Disclaimer

The information provided in this secur 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