



# FreeScout Stored XSS vulnerability in mailbox auto-reply: payload reaches every customer's email client (no CSP), bypassing strip\_tags validator with mixed text+HTML content

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-41904
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 19:16:01 UTC
<b>Updated</b>	2026-05-07 20:16:43 UTC
<b>Description</b>	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.217, a user with up

## Risk And Classification

**Primary CVSS:** v3.1 7.6 HIGH from security-advisories@github.com

**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N

**EPSS:** 0.000320000 probability, percentile 0.094980000 (date 2026-05-12)

**Problem Types:** CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N
3.1	CNA	DECLARED	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Freescout-help-desk	Freescout	affected < 1.8.217	Not specified

### References

Reference	Source	Link	Tags
github.com/freescout-help-desk/freescout/releases/tag/1.8.217	security-advisories@github.com	github.com	
github.com/freescout-help-desk/freescout/security/advisories/GHSA-q3fh-r...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)