



# FreeScout's Mass Assignment in Mailbox Connection Settings Enables Silent Email Exfiltration

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

## Summary

<b>CVE</b>	CVE-2026-40569
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 17:16:55 UTC
<b>Updated</b>	2026-04-21 18:16:50 UTC
<b>Description</b>	FreeScout is a free self-hosted help desk and shared mailbox. Versions prior to 1.8.213 have a mass assignment vulnerabi

## Risk And Classification

**Primary CVSS:** v3.1 9 CRITICAL from security-advisories@github.com

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

**Problem Types:** CWE-284 | CWE-915 | CWE-284 CWE-284: Improper Access Control | CWE-915 CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9	CRITICAL	<b>CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L</b>
3.1	CNA	DECLARED	9	CRITICAL	<b>CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**High**

User Interaction

**None**

Scope

**Changed**

Confidentiality

**High**

Integrity

High

Availability

Low

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Freescout-help-desk</a>	<a href="#">Freescout</a>	affected < 1.8.213	Not specified

#### References

Reference	Source	Link
<a href="https://github.com/freescout-help-desk/freescout/releases/tag/1.8.213">github.com/freescout-help-desk/freescout/releases/tag/1.8.213</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/freescout-help-desk/freescout/commit/f45b9105d43b0352c08fcca1...">github.com/freescout-help-desk/freescout/commit/f45b9105d43b0352c08fcca1...</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/freescout-help-desk/freescout/security/advisories/GHSA-hmqm-3...">github.com/freescout-help-desk/freescout/security/advisories/GHSA-hmqm-3...</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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)