



# FreeScout: Host Header Injection Leading to External Resource Loading and Open Redirect in FreeScout

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

## Summary

<b>CVE</b>	CVE-2026-34442
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 22:16:19 UTC
<b>Updated</b>	2026-04-01 19:49:03 UTC
<b>Description</b>	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.211, host header m

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000390000 probability, percentile 0.117650000 (date 2026-04-01)

**Problem Types:** CWE-20 | CWE-601 | CWE-829 | CWE-20 CWE-20: Improper Input Validation | CWE-601 CWE-601: URL Redirection to Untrusted Site ('Open Redirect') | CWE-829 CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	security-advisories@github.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freescout	Freescout	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Freescout-help-desk	Freescout	affected < 1.8.211	Not specified

#### References

Reference	Source	Link
github.com/freescout-help-desk/freescout/commit/889d75c8e3c15e6a7ddb6a4d...	security-advisories@github.com	github.com
github.com/freescout-help-desk/freescout/security/advisories/GHSA-822g-7...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/freescout-help-desk/freescout/releases/tag/1.8.211	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)