



# CVE-2026-38566

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

## Summary

<b>CVE</b>	CVE-2026-38566
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-11 18:16:32 UTC
<b>Updated</b>	2026-05-12 14:17:02 UTC
<b>Description</b>	HireFlow v1.2 does not implement CSRF token validation on any state-changing POST endpoint. All forms (password chan

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from ADP

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

**Problem Types:** CWE-352 | n/a | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source
github.com/StratonWebDesigners/HireFlow	cve@mitre.org
www.sourcecodester.com/python/18688/hireflow-%E2%80%93-complete-interview-management...	cve@mitre.org
github.com/hijackedamygdala/CVE-Disclosures/tree/main/HireFlow/CVE-2026-...	134c704f-9b21-4f2e-91b3-4a467353bcc
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)

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