



Open WebUI: Stored Cross-Site Scripting In Profile Picture

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-45299 |
| State | PUBLISHED |
| Assigner | GitHub_M |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-15 22:16:53 UTC |
| Updated | 2026-05-15 22:16:53 UTC |
| Description | Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, the profile_image |

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from security-advisories@github.com

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

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 | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N |
| 3.1 | CNA | DECLARED | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Severity: **Low**

Availability: **None**

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------|------------|------------------|---------------|
| CNA | Open-webui | Open-webui | affected < 0.8.0 | Not specified |

References

| Reference | Source | Link | Tags |
|--|--------------------------------|---|------------|
| github.com/open-webui/open-webui/security/advisories/GHSA-6gh2-q7cp-9qf6 | security-advisories@github.com | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). 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