



# WordPress ProfileGrid plugin <= 5.9.5.7 - Reflected Cross Site Scripting (XSS) vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-4957
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-26 09:15:32 UTC
<b>Updated</b>	2026-04-01 17:25:29 UTC
<b>Description</b>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss ProfileGrid

## Risk And Classification

**EPSS:** 0.000330000 probability, percentile 0.096590000 (date 2026-04-02)

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

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Metagauss</a>	<a href="#">ProfileGrid</a>	affected 5.9.5.7 custom	Not specified

## References

Reference	Source	Link	Tags
<a href="https://patchstack.com/database/Wordpress/Plugin/profilegrid-user-profiles-groups-an...">patchstack.com/database/Wordpress/Plugin/profilegrid-user-profiles-groups-an...</a>	<a href="mailto:audit@patchstack.com">audit@patchstack.com</a>	<a href="https://patchstack.com">patchstack.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ana

## Vendor Comments And Credit

Discovery Credit

**CNA:** Mohammed Ahmed Abd Elnabi | Patchstack Bug Bounty Program (en)

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](#)**