



WordPress Paid Memberships Pro – Payfast Gateway Add On plugin <= 1.4.1 - Sensitive Data Exposure via Log File vulnerability

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

Summary

CVE	CVE-2024-30514
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-29 16:15:10 UTC
Updated	2026-04-28 19:24:07 UTC
Description	Insertion of Sensitive Information into Log File vulnerability in Paid Memberships Pro Paid Memberships Pro – Payfast Gate

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.003260000 probability, percentile 0.555570000 (date 2026-04-28)

Problem Types: CWE-532 | CWE-532 CWE-532 Insertion of Sensitive Information into Log File

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Paid Memberships Pro	Paid Memberships Pro Payfast Gateway Add On	affected n/a 1.4.1 custom	Not specified
ADP	Paidmembershipspro	Paid Memberships Pro	affected 1.4.1 custom	Not specified

References

Reference

[WordPress Paid Memberships Pro – Payfast Gateway Add On plugin <= 1.4.1 - Sensitive Data Exposure via Log File vulnerability - Patchstack](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

CNA: [Joshua Chan \(Patchstack Alliance\)](#) (en)

Additional Advisory Data

Solutions

CNA: Update to 1.4.2 or a higher version.

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](#)

