



WordPress Hercules Core plugin <= 7.4 - Server Side Request Forgery (SSRF) vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-63010
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-09 16:18:06 UTC
Updated	2026-04-27 19:16:17 UTC
Description	Server-Side Request Forgery (SSRF) vulnerability in ThemesInflow Hercules Core hercules-core allows Server Side Reque

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from audit@patchstack.com

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

EPSS: 0.000420000 probability, percentile 0.127200000 (date 2026-04-27)

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ThemesInflow	Hercules Core	affected 7.4 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/hercules-core/vulnerability/wordpre...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

Vendor Comments And Credit

Discovery Credit

CNA: Bonds | Patchstack Bug Bounty Program (en)

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