



WordPress YITH WooCommerce Wishlist plugin <= 4.12.0 - Insecure Direct Object References (IDOR) vulnerability

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

Summary

CVE	CVE-2026-27329
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 09:16:27 UTC
Updated	2026-05-07 09:16:27 UTC
Description	Authorization Bypass Through User-Controlled Key vulnerability in YITH YITH WooCommerce Wishlist allows Exploiting Inc

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:N/I:L/A:N

Problem Types: CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

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:N/I:L/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	YITH	YITH WooCommerce Wishlist	affected n/a 4.12.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/wordpress/plugin/yith-woocommerce-wishlist/vulnerabi...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: PPzzAArr | Patchstack Bug Bounty Program (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress YITH WooCommerce Wishlist Plugin to the latest available version (at least 4.13.0).

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