



WordPress YITH WooCommerce Product Add-Ons Plugin <= 4.3.0 is vulnerable to PHP Object Injection

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

Summary

CVE	CVE-2023-49777
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-31 11:15:08 UTC
Updated	2026-04-28 19:22:25 UTC
Description	Deserialization of Untrusted Data vulnerability in YITH YITH WooCommerce Product Add-Ons.This issue affects YITH Woo

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.003830000 probability, percentile 0.596290000 (date 2026-04-28)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yithemes	Yith Woocommerce Product Add-ons	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	YITH	YITH WooCommerce Product Add-Ons	affected n/a 4.3.0 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/yith-woocommerce-product-add-ons/wordp...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Rafie Muhammad (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 4.3.1 or a higher version.

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

[site](#). 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