WPshop 2 – E-Commerce 2.0.0 - 2.6.0 - Insecure Direct Object Reference to Authenticated (Subscriber+) Arbitrary User Key Generation

Authorization Bypass Through User-Controlled Key

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

CVE	CVE-2025-3853
CVSS	6.5 (Medium)
Publicly Published	May 6, 2025
Last Updated	May 7, 2025
Researcher	kr0d

Description

The WPshop 2 – E-Commerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions 2.0.0 to 2.6.0 via the callback_generate_api_key() due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create valid API keys on behalf of other users.

References

- plugins.trac.wordpress.org

Share

Facebook Twitter LinkedIn Email

Vulnerability Details for WPshop 2 – E-Commerce

WPshop 2 – E-Commerce

Software Type	Plugin
Software Slug	wpshop (view on wordpress.org)
Patched?	✖ No
Remediation	No known patch available. Please review the vulnerability's details in depth and employ mitigations based on your organization's risk tolerance. It may be best to uninstall the affected software and find a replacement.

This record contains material that is subject to copyright.

publicly display, publicly perform, sublicense, and distribute this software vulnerability information. Any copy of the software vulnerability information you make for such purposes is authorized provided that you include a hyperlink to this vulnerability record and reproduce Defiant's copyright designation and this license in any such copy. Read more.

Have information to add, or spot any errors? Contact us at wfi-support@wordfence.com so we can make any appropriate adjustments.