4Jawaly Security Advisory - CVE-2026-7630
==========
Generated: 2026-05-02 20:44 UTC
Advisory URL: https://www.4jawaly.com/innoshop-improper-authentication-installation-endpoint-vulnerability/

CVE ID: CVE-2026-7630
Severity: HIGH
CVSS Score: 7.3
CWE: CWE-287

EXECUTIVE SUMMARY
A vulnerability has been found in innocommerce InnoShop up to 0.7.8. The affected element is the function InstallServiceProvider::boot of the file innopacks/install/src/InstallServiceProvider.php of the component Installation Endpoint. The manipulation leads to improper authentication. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The identifier of the patch is 45758e4ec22451ab944ae2ae826b1e70f6450dc9. It is recommended to apply a patch to fix this issue.

AFFECTED PRODUCT / COMPONENT
See vendor advisory and affected component details.

RISK FOR HOSTING AND SERVER OPERATORS
This vulnerability may affect websites, hosting panels, plugins, or server-side components. Operators should identify exposed installations, review access controls, inspect logs for suspicious activity, and apply the vendor fix as soon as it becomes available.

RECOMMENDED ACTIONS
1. Update the affected software to the latest patched version. 2. Restrict administrative access and review user privileges. 3. Monitor web server and application logs for exploitation attempts. 4. Apply WAF or virtual patching rules where available. 5. Keep backups and verify recovery procedures.

REFERENCES
- https://github.com/innocommerce/innoshop/
- https://github.com/innocommerce/innoshop/commit/45758e4ec22451ab944ae2ae826b1e70f6450dc9
- https://github.com/innocommerce/innoshop/issues/314
- https://github.com/innocommerce/innoshop/issues/314issuecomment-4357464458
- https://vuldb.com/submit/806484
- https://vuldb.com/vuln/360576
- https://vuldb.com/vuln/360576/cti

Prepared by 4Jawaly - Security and Web Hosting Alerts