Posted Date: 2026/07/27

Vulnerability AlertTwo High-Risk Security Vulnerabilities Exist in WordPress (CVE-2026-60137 and CVE-2026-63030), Please Confirm and Patch as Soon as Possible

- Subject: Vulnerability AlertTwo High-Risk Security Vulnerabilities Exist in WordPress (CVE-2026-60137 and CVE-2026-63030), Please Confirm and Patch as Soon as Possible

- Description:
  - Forwarded from National Information Security Analysis and Sharing Center Information Security Alert NISAC-200-202607-00000006
  - Researchers have discovered two high-risk security vulnerabilities in WordPress (CVE-2026-60137 and CVE-2026-63030), which are classified as SQL Injection and a REST API batch endpoint routing misinterpretation issue, respectively. Among them, CVE-2026-60137 has already been exploited by hackers. Please verify and patch as soon as possible.
  - CVE-2026-60137: When a plugin or theme passes untrusted input into affected functions, it may lead to SQL injection.
  - CVE-2026-63030: An unauthenticated remote attacker could exploit the REST API batch endpoint routing misinterpretation issue, combined with CVE-2026-60137, to execute SQL injection and subsequently execute arbitrary code on the affected system.
- Affected Platforms:
  - WordPress versions 6.8.0 to 6.8.5
  - WordPress versions 6.9.0 to 6.9.4
  - WordPress versions 7.0.0 to 7.0.1
- Recommendations:
  - Official fix updates for these vulnerabilities have been released. Please upgrade to the following versions and refer to the official instructions to update: https://wordpress.org/news/2026/07/wordpress-7-0-2-release/
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-60137
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-63030
  3. https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

Computer and Communication Center
Network System Division

From:
https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260727_22

Last update: **2026/07/27 14:40**