Posting Date: 2026/07/17

Vulnerability AlertMultiple high-risk security vulnerabilities (CVE-2026-12044 to CVE-2026-12050) exist in pgAdmin 4. Please confirm and patch them as soon as possible

- Subject: Vulnerability AlertMultiple high-risk security vulnerabilities (CVE-2026-12044 to CVE-2026-12050) exist in pgAdmin 4. Please confirm and patch them as soon as possible.

- Description:
  - Forwarded from the National Information Security Analysis Center (NISAC) security alert NISAC-200-202607-00000002.
  - Researchers have discovered multiple high-risk security vulnerabilities (CVE-2026-12044 to CVE-2026-12050) in pgAdmin 4. The most critical one is CVE-2026-12046, an Insecure Deserialization vulnerability. When the product is running in server mode, and an attacker knows the Flask SECRET_KEY of pgAdmin and has write permissions to pgAdmin's Session directory, they can exploit this vulnerability to execute arbitrary code. Please confirm and apply the patches as soon as possible.
- Affected Platforms:
  - pgAdmin 4 versions 1.0 to 9.15
- Recommended Actions:
  - The vendor has released security updates to address these vulnerabilities. Please refer to the official announcement to perform the update. The URL is as follows: https://www.postgresql.org/about/news/pgadmin-4-v916-released-3324/
- Reference Information:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-12044
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-12045
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-12046
  4. https://nvd.nist.gov/vuln/detail/CVE-2026-12047
  5. https://nvd.nist.gov/vuln/detail/CVE-2026-12048
  6. https://nvd.nist.gov/vuln/detail/CVE-2026-12049
  7. https://nvd.nist.gov/vuln/detail/CVE-2026-12050
  8. https://www.postgresql.org/about/news/pgadmin-4-v916-released-3324/

Computer and Communication Center
Network Systems Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260717_21

Last update: **2026/07/17 10:47**