Date Posted: 2026/02/25

[Attack Warning] High-Risk Security Vulnerability Found in BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) (CVE-2026-1731), Please Confirm and Patch Immediately

- Subject Explanation: [Attack Warning] High-Risk Security Vulnerability Found in BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) (CVE-2026-1731), Please Confirm and Patch Immediately

- Content Description:
  - Forwarding National Information Security Analysis and Sharing Center (NISAC) Alert NISAC-200-202602-00000092
  - Researchers have discovered an OS Command Injection vulnerability (CVE-2026-1731) in BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA). An unauthenticated remote attacker could inject arbitrary operating system commands and execute them on the server.
  - This vulnerability has already been exploited by hackers; please confirm and patch immediately.
- Impacted Platforms:
  - Remote Support 25.3.1 and earlier versions
  - Privileged Remote Access 24.3.4 and earlier versions
- Suggested Measures:
  - The official vendor has released a repair update for the vulnerability; please refer to the official instructions to update. The URL is as follows: https://www.beyondtrust.com/trust-center/security-advisories/bt26-02
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-1731
  2. https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

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:20260225_24

Last update: **2026/02/25 15:43**