Date Posted: 2025/08/04

[Vulnerability Alert] High-Risk Security Vulnerabilities (CVE-2025-37102 and CVE-2025-37103) Exist in HPE's Networking Instant On Wireless Access Points. Please Confirm and Patch as Soon as Possible

- Subject: [Vulnerability Alert] High-Risk Security Vulnerabilities (CVE-2025-37102 and CVE-2025-37103) Exist in HPE's Networking Instant On Wireless Access Points. Please Confirm and Patch as Soon as Possible
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202507-00000230
  - Researchers have discovered two high-risk security vulnerabilities (CVE-2025-37102 and CVE-2025-37103) in HPE's Networking Instant On wireless access points. The vulnerability types are OS Command Injection and Use of Hard-coded Credentials, respectively. The former allows a remote attacker with administrative privileges to inject and execute arbitrary operating system commands on the device, while the latter allows an unauthenticated remote attacker to use fixed account credentials to log in to the system with administrator privileges. Please confirm and patch as soon as possible.
- Affected Platforms:
  - HPE Networking Instant On wireless access point software versions 3.20.1 (inclusive) and below
- Recommended Action:
  - The official site has released a fix for the vulnerabilities. Please refer to the official instructions for updating, the URL is as follows: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04894en_us&docLocale=en_US
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-37102
  2. https://nvd.nist.gov/vuln/detail/CVE-2025-37103
  3. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04894en_us&docLocale=en_US

Computer and Communications Center
Network Systems Group

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250804_07

Last update: **2025/08/04 18:34**