Date Posted: 2026/03/19

[Vulnerability Alert] High-Risk Security Vulnerability Found in Ivanti Endpoint Manager (CVE-2026-1603), Please Confirm and Patch Immediately

- Subject Explanation: [Vulnerability Alert] High-Risk Security Vulnerability Found in Ivanti Endpoint Manager (CVE-2026-1603), Please Confirm and Patch Immediately

- Content Description:
  - Forwarding National Information Security Analysis and Sharing Center (NISAC) Alert NISAC-200-202603-00000007
  - Researchers have discovered an Authentication Bypass vulnerability (CVE-2026-1603) in Ivanti Endpoint Manager. An unauthenticated remote attacker could obtain specific authentication data. This vulnerability has already been exploited by hackers; please confirm and patch immediately.
- Impacted Platforms:
  - Ivanti Endpoint Manager 2024 SU4 SR1 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://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-1603
  2. https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US

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:20260319_24

Last update: **2026/03/19 15:52**