**Date Posted: 2026/03/19**

# [Vulnerability Alert] Critical Security Vulnerability Found in Zoom Workplace for Windows (CVE-2026-30903)

- Subject Explanation: [Vulnerability Alert] Critical Security Vulnerability Found in Zoom Workplace for Windows (CVE-2026-30903)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000009
  - Recently, Zoom released a critical security advisory for Zoom Workplace for Windows (CVE-2026-30903, CVSS: 9.6). This vulnerability exists in the mail feature. Because file names or paths can be externally controlled, it may allow an unauthenticated attacker to access the system over the network and escalate privileges.
- Impacted Platforms:
  - Zoom Workplace for Windows versions prior to 6.6.0
  - Zoom Workplace VDI Client for Windows versions prior to 6.4.17, 6.515, and 6.6.10
- Suggested Measures:
  - Please patch according to the solutions released on the official website: https://www.zoom.com/en/trust/security-bulletin/zsb-26005/
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10758-31469-1.html

---

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_22**

Last update: **2026/03/19 15:38**