

POSTING DATE: 2026/01/23

[VULNERABILITY ALERT] Zoom Node Multimedia Routers Contain a Critical Security Vulnerability (CVE-2026-22844)

- Subject: [VULNERABILITY ALERT] Zoom Node Multimedia Routers Contain a Critical Security Vulnerability (CVE-2026-22844)
- Content Description:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202601-00000018
 - Zoom Node Multimedia Routers (MMRs) are core modules of a hybrid cloud solution provided by Zoom, primarily used to handle meeting media traffic, enhance bandwidth efficiency, and reduce latency. Recently, Zoom released a critical security advisory (CVE-2026-22844, CVSS: 9.9). This is a command injection vulnerability where meeting participants may execute remote code on MMRs via network access.
- Affected Platforms:
 - Zoom Node Meetings Hybrid (ZMH) MMR module: Versions prior to 5.2.1716.0 (exclusive)
 - Zoom Node Meeting Connector (MC) MMR module: Versions prior to 5.2.1716.0 (exclusive)
- Recommended Actions:
 - Please perform patching based on the solutions released on the official website: <https://www.twcert.org.tw/tw/cp-169-10648-b83d7-1.html>
- Reference Material:
 - 1 <https://www.twcert.org.tw/tw/cp-169-10648-b83d7-1.html>

Computer and Communication Center
Network Systems Division, Respectfully

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260123_04

Last update: **2026/01/23 10:57**

