Posting date: 2025/08/11

Vulnerability Alert Microsoft Exchange Server has a major security vulnerability (CVE-2025-53786)

- Subject: Vulnerability Alert Microsoft Exchange Server has a major security vulnerability (CVE-2025-53786)
- Details:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202508-00000004
  - Microsoft has issued a major security vulnerability announcement (CVE-2025-53786, CVSS: 8.0) for its Exchange Server product. This vulnerability allows an attacker with administrative privileges to elevate their privileges in hybrid cloud-on-premise environments. Currently, log monitoring tools in cloud environments cannot record malicious activity related to this vulnerability.
  - A related PoC for this vulnerability was publicly demonstrated at the recent Black Hat conference in the United States, which may accelerate subsequent exploitation by attackers. Microsoft has released security updates and provided temporary mitigation measures. It is recommended to take temporary mitigation measures as soon as possible to prevent potential attacks exploiting this vulnerability.
- Affected Platforms:
  - Microsoft Exchange Server Subscription Edition RTM versions 15.02.0.0 to 15.02.2562.017
  - Microsoft Exchange Server 2016 Cumulative Update 23 versions 15.01.0 to 15.01.2507.055
  - Microsoft Exchange Server 2019 Cumulative Update 14 versions 15.02.0.0 to 15.02.1544.025
  - Microsoft Exchange Server 2019 Cumulative Update 15 versions 15.02.0 to 15.02.1748.024
- Recommended Actions:
  - Patch according to the solution released on the official website: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53786
- References:
  - 1 https://www.twcert.org.tw/tw/cp-169-10316-60f9c-1.html

Computer and Communications Center
Network Systems Group, Regards

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250811_01

Last update: **2025/08/11 15:25**