Posted Date: 2025/10/29

[Vulnerability Alert] Windows Server Update Services has a high-risk security vulnerability (CVE-2025-59287), please confirm and patch as soon as possible

- Subject: [Vulnerability Alert] Windows Server Update Services has a high-risk security vulnerability (CVE-2025-59287), please confirm and patch as soon as possible

- Content:
    - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202510-00000233
    - Researchers have discovered an insecure Deserialization of Untrusted Data vulnerability (CVE-2025-59287) in Windows Server Update Services. An unauthenticated remote attacker can execute arbitrary code with system privileges by sending a specially crafted event to the WSUS server. This vulnerability has already been exploited by hackers, so please confirm and patch it as soon as possible.
- Affected Platforms:
    - Windows Server 2025 (Server Core installation)
    - Windows Server 2025
    - Windows Server 2022, 23H2 Edition (Server Core installation)
    - Windows Server 2022 (Server Core installation)
    - Windows Server 2022
    - Windows Server 2019 (Server Core installation)
    - Windows Server 2019
    - Windows Server 2016 (Server Core installation)
    - Windows Server 2016
    - Windows Server 2012 R2 (Server Core installation)
    - Windows Server 2012 R2
    - Windows Server 2012 (Server Core installation)
    - Windows Server 2012
- Recommended Measures:
    - The official source has released a security update for the vulnerability; please refer to the official instructions for update at the following URL:
    https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287
- References:
    1. https://nvd.nist.gov/vuln/detail/CVE-2025-59287
    2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287
    3. https://www.cisa.gov/news-events/alerts/2025/10/24/microsoft-releases-out-band-security-update-mitigate-windows-server-update-service-vulnerability-cve
    4. https://www.helpnetsecurity.com/2025/10/24/wsus-vulnerability-cve-2025-59287-exploited/

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:20251029_01

Last update: **2025/10/29 15:24**

Computer and Communications Center
Network Systems Group