GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

28 October 2025

Advisory 108: Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability

Release Date: 24th of October 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-59287 – is a **critical, unauthenticated remote code execution (RCE)** vulnerability in Windows Server Update Services (WSUS) caused by unsafe deserialization of untrusted data in WSUS web services.

What are the Systems affected?

Affected:

WSUS Server Role on supported Windows Server releases (examples called out in vendor advisories: **Windows Server 2012 / 2012 R2, 2016, 2019, 2022,** and **2025**) where the WSUS role is enabled and the server has not applied Microsoft's October 2025 patch update. Systems without the WSUS role enabled are not vulnerable.

What does this mean?

How attackers exploit this vulnerability (attack vector)

Remote, unauthenticated network attack – an attacker sends crafted HTTP requests to WSUS's reporting /web endpoints (observed against default WSUS ports 8530/8531) that exploit unsafe deserialization to execute arbitrary code as SYSTEM on the WSUS server.

Mitigation process

CERTVU recommend:

1. Immediate Patching - Apply Microsoft's October 2025 security update
2. If for some reasons you cannot block immediately:
    - Remove/disable the WSUS Server Roles on hosts that do not need it
    - Block network access to WSUS management ports (TCP 8530 and 8531)

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-59287