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

21 May 2026

Advisory 143: Microsoft Windows Buffer Overflow Vulnerability.

Release Date: 20th May 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications 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-2008-4250 is a critical remote code execution (RCE) vulnerability in the Microsoft Windows Server Service. The flaw is caused by an improperly handled RPC request resulting in a stack-based buffer overflow.

The vulnerability became widely known through exploitation by the **Conficker** worm and is associated with Microsoft Security Bulletin MS08-067

What are the systems affected?

The vulnerability affects older Microsoft Windows systems, including:

- Windows 2000
- Windows XP
- Windows Vista
- Windows Server 2003

- Windows Server 2008 (certain configurations)

Because vCenter centrally manages virtual infrastructure, it is a high-value target.

What does this mean?

This vulnerability is **wormable**, meaning it can spread automatically across networks without user interaction.

Typical exploitation flow:

1. **Target scanning**
   - Attackers scan for systems exposing SMB/RPC services (TCP 445)**.**
2. **Malicious RPC request sent**
   - A specially crafted network packet is delivered to the Windows Server Service.
3. **Buffer overflow triggered**
   - Improper bounds checking causes a stack overflow in memory.
4. **Arbitrary code execution**
   - The attacker executes malicious code with SYSTEM privileges.
5. **Automated propagation**
   - Malware may scan for additional vulnerable systems and self-propagate.

Mitigation process

CERTVU recommends the following:

Apply Microsoft Security Updates (Critical)

- Install security update MS08-067 immediately on vulnerable systems
- Ensure all Windows systems are fully patched

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2008-4250
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
4. https://support.microsoft.com/en-us/topic/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execution-ac7878fc-be69-7143-472d-2507a179cd15

.