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

23 April 2026

Advisory 136: Microsoft Office Remote Code Execution (CVE-2009-0238).

Release Date: 14th April 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-2009-0238 is a critical remote code execution vulnerability (CVSS ~9.3) in Microsoft Windows Internet Printing service (MS08-067-related RPC component exposure). It is caused by a stack-based buffer overflow in the handling of RPC requests over SMB (Server Message Block).

The flaw allows an attacker to send a specially crafted network request that overflows memory buffers in the Windows RPC service, enabling arbitrary code execution at SYSTEM level.

What are the systems affected?

The vulnerability affects older Microsoft Windows operating systems, including:

- Windows 2000
- Windows XP (all editions at the time)
- Windows Server 2003
- Windows Vista (pre-patched systems)

- Windows Server 2008 (pre-patched systems)

What does this mean?

Typical exploitation flow:

1. **Network scanning**
   - Attackers scan networks for systems exposing **SMB (TCP port 445)**.
2. **Crafted RPC request**
   - A specially designed RPC packet is sent to the Windows Server Service.
3. **Buffer overflow triggered**
   - The service fails to properly validate input, causing a **stack-based buffer overflow**.
4. **Remote code execution**
   - Attacker overwrites memory and executes code with **SYSTEM privileges**.
5. **Worm propagation (common in real attacks)**
   - Malware automatically spreads to other vulnerable systems across the network.

Successful exploitation of this vulnerability may allow attackers to:

- Execute arbitrary code remotely with SYSTEM privileges
- Install malware or worm payloads
- Fully compromise affected systems
- Spread laterally across internal networks
- Disrupt services and cause large-scale outages

Mitigation process

CERTVU recommends the following:

1. Apply Security Patches (Critical)

- Install Microsoft security update MS08-067 (MS09-023 and later cumulative fixes depending on system state)
- Ensure all legacy systems are fully patched or upgraded

2. Disable or Restrict SMB (TCP 445)

- Block SMB traffic at network boundaries
- Disable SMBv1 on legacy systems where possible
- Restrict access to trusted internal hosts only

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2009-0238
3. https://nvd.nist.gov/vuln/detail/cve-2009-0238
4. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067