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 130: Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability (CVE-2012-1854).

Release Date: 13th 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-2012-1854 is a critical remote code execution vulnerability in Microsoft Windows**,** specifically within the Microsoft XML Core Services (MSXML) component used by Internet Explorer and other applications.

The flaw is caused by improper handling of objects in memory (use-after-free / memory corruption) when processing specially crafted web content. This allows attackers to corrupt memory and execute arbitrary code.

What are the systems affected?

The following version affected;

The vulnerability affects older Microsoft platforms, including:

- Microsoft Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

And associated components:

- Microsoft XML Core Services (MSXML) versions 3.0, 4.0, 5.0, and 6.0
- Internet Explorer (various versions at the time)

Note: These systems are now **end-of-life (EOL)** and no longer receive security updates, increasing risk if still in use.

What does this mean?

Typical attack flow:

1. **Malicious webpage or content delivery**
    - Attackers host a specially crafted website or inject malicious code into legitimate sites.
2. **User interaction**
    - The victim visits the malicious webpage using Internet Explorer or an application leveraging MSXML.
3. **Triggering the vulnerability**
    - The crafted content causes MSXML to improperly handle objects in memory.
4. **Memory corruption (use-after-free)**
    - The application accesses freed memory, allowing attacker-controlled data to be executed.
5. **Remote code execution**
    - The attacker executes arbitrary code in the context of the logged-in user.

Attack vectors:

- Malicious websites
- Compromised legitimate websites (drive-by downloads)
- Phishing emails containing malicious links

Successful exploitation of **CVE-2012-1854** may allow attackers to:

- Execute arbitrary code on the target system
- Install malware or spyware
- Steal sensitive information
- Take full control of the affected system (if user has admin privileges)
- Use the system as a foothold for further network compromise

Mitigation process

CERTVU recommends the following:

1. Apply Microsoft Security Updates

- Install updates provided in Microsoft Security Bulletin MS12-043 (June 2012).
- Ensure all MSXML components are updated to patched versions.

2. Upgrade or Replace Legacy Systems (Critical)
3. Use Modern Browsers

- Avoid legacy Internet Explorer versions.
- Use modern browsers with stronger security controls and sandboxing.

4. Apply Least Privilege

- Operate systems using non-administrative user accounts to reduce impact.

5. Network and Endpoint Protection

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2012-1854
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-043
4. https://support.microsoft.com/en-us/topic/ms12-043-description-of-the-security-update-for-xml-core-services-5-0-when-it-is-installed-together-with-office-2007-office-compatibility-pack-office-word-viewer-expression-web-or-expression-web-2-august-14-2012-b67932c4-637f-f75e-4784-083e82818920

.