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 145: Microsoft Internet Explorer Use-After-Free 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-2010-0249 is a critical remote code execution (RCE) vulnerability in Microsoft Internet Explorer. The flaw is caused by **a** memory corruption/use-after-free vulnerability in the way Internet Explorer handles certain HTML objects and cascading style sheets

When a user visits a specially crafted malicious webpage, Internet Explorer may improperly access freed memory, allowing attackers to execute arbitrary code on the victim's system.

What are the systems affected?

The vulnerability affects:

- **Microsoft Internet Explorer 6, 7, and 8**
- Supported Microsoft Windows systems at the time, including:

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

What does this mean?

Typical exploitation flow:

1. **Malicious website preparation**
    - The attacker creates a webpage containing specially crafted HTML/CSS and JavaScript.
2. **Victim lured to the site**
    - Delivery methods include:
        - Phishing emails
        - Instant messaging links
        - Compromised legitimate websites
3. **Memory corruption triggered**
    - Internet Explorer improperly handles specific objects and accesses invalid memory.
4. **Use-after-free exploitation**
    - The attacker manipulates freed memory to redirect execution flow.
5. **Remote code execution**
    - Malicious code runs with the privileges of the logged-in user.

Mitigation process

CERTVU recommends the following:

Apply Microsoft Security Updates (Critical)

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2010-0249

.