**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

8 October 2025

Advisory 102: Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability

Release Date: 06th 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-2010-3962 is a **use-after-free / uninitialized memory corruption** vulnerability in Microsoft Internet Explorer (IE) that was disclosed in November 2010. The vulnerability allows a specially crafted web page to trigger improper handling of an object (via CSS token sequences and the clip attribute), leading to memory corruption and potential remote code execution in the context of the user viewing the page.

What are the Systems affected?

Affected:

Internet Explorer 6,7, and 8 (on affected Windows platforms at the time.

What does this mean?

Attackers can take advantage of this exploit or attack vector by

- Remote, client-side attack: An attacker hosts or injects a specially crafted web page where victims using a vulnerable IE (Internet Explorer) version loads the page, the exploit triggers the use-after-free condition and achieves memory corruption that can be chained to execute arbitrary code. An attacker could also weaponize this inside HTML email/Word documents in some attack chains.
- Exploit in the Wild: this vulnerability was actively exploited in November 2010 and remained a common target for obfuscated web exploit kits and targeted client-side attacks.

Mitigation process

CERTVU recommend:

1. Patch immediately – apply Microsoft's security update referenced in MS10-090

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2010-3962
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-090