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

9 October 2025

Advisory 105: Microsoft Windows Remote Code Execution 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-2011-3402: is a remote code execution vulnerability in the **TrueType font parsing** engine (win32k.sys) that allows specially crafted font data in a web page or Office document to execute code in kernel mode

What are the Systems affected?

Windows versions affected include:

- Windows XP (SP2/SP3),
- Windows Server 2003 (SP2),
- Windows Vista (SP2),
- Windows Server 2008 (SP2 / R2),
- Windows 7 (Gold / SP1) and
- corresponding server builds that were supported in 2011 — i.e., systems that did not receive the MS11-087 update are vulnerable.

What does this mean?

Allows remote attackers to execute arbitrary code via crafted font data in a Word document or web page, as exploited in the wild in November 2011 by Duqu, aka “TrueType Font Parsing Vulnerability.”

Mitigation process

CERTVU recommend:

Apply Microsoft patching updates immediately. Install Microsoft security update MS11-087 (December 13, 2011) which addresses CVE-2011-3402.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2011-3402
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-087
4. https://exploitshop.wordpress.com/2012/01/18/ms11-087-aka-duqu-vulnerability-in-windows-kernel-mode-drivers-could-allow-remote-code-execution/