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

30 January 2026

Advisory 118: Microsoft Office Security Feature Bypass Vulnerability

Release Date: 26th January 2026
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-2026-21509 is a **high-severity security feature bypass vulnerability** in Microsoft Office caused by reliance on untrusted input in security decisions. It allows attackers to bypass built-in protections (e.g., OLE/COM security controls) when a user opens a specially crafted Office document.

What are the systems affected?

The vulnerability affects multiple Microsoft Office products, including:

- Microsoft Office 2016 and 2019
- Microsoft Office LTSC 2021 and 2024
- Microsoft 365 Apps (Enterprise)

What does this mean?

Attackers exploit CVE-2026-21509 by:

- Sending specially crafted malicious Office files via phishing or social engineering.
- Tricking users into opening the document, which bypasses Office security protections.
- Executing unsafe embedded objects or payloads, enabling malware delivery, data access, or further system compromise.

  This vulnerability is particularly dangerous because it is **actively exploited in the wild**

Mitigation process

CERTVU recommend:

- Immediately applying Microsoft's emergency security updates for all affected Office versions.
- Updating Office to the latest supported version and restarting applications to enable protections.
- Implementing temporary mitigations (e.g., registry or configuration changes) where patches are not yet deployed.

Reference

.

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-21509