

**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



**GOVERNEMENT 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

14 October 2026

**Advisory 355: Microsoft Windows Shell Mark of the Web Security Feature
Bypass Vulnerability - Actively Exploited Zero-Day (CVE-2026-96951).**

Release Date: 13th October 2026

Impact: **HIGH**

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 product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-96951 is a security feature bypass vulnerability in Microsoft Windows Shell that was exploited in the wild as a zero-day before Microsoft released a fix in its October 2026 Patch Tuesday update. It lets a malicious file avoid the Mark of the Web (MOTW) protections, so Windows does not show the usual SmartScreen and Protected View warnings when the file is opened. It is rated CVSS 8.8 (Important). An attacker needs the user to open the file, typically one delivered by email, a messaging app or a download, so social engineering is required.

What are the systems affected?

Supported Windows client and server versions that have not installed the October 2026 security updates are affected, including:

- Windows 11, including version 24H2, and Windows 10
- Windows Server 2016 and later supported Windows Server releases

Not affected / patched version:

- The October 2026 cumulative or security-only updates for each version. Reported examples of fixed builds are Windows 11 24H2 build 10.0.26100.9711 and Windows 10 1607 /

Windows Server 2016 build 10.0.14393.9612; confirm the exact build for your version in Microsoft's Security Update Guide

What does this mean?

Successful exploitation may allow attackers to:

- Open a malicious file without the normal SmartScreen and Mark of the Web warnings, which removes a key defence against phishing attachments
- Allow malware, scripts or shortcuts delivered by email, chat or web download to run with less user suspicion
- Serve as the first step of a longer attack, for example to deliver ransomware or an information stealer

Mitigation process

CERTVU recommends the following:

1. Install the October 2026 updates

Apply the October 2026 Windows security updates to all workstations and servers, and use patch management tools to check that they are installed.

2. Prioritize high-risk users

Patch devices of staff who handle external email and files first, such as executives, finance, and administrators.

Reference

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951>
2. <https://www.tenable.com/blog/microsofts-october-2026-patch-tuesday-addresses-1407-cves-cve-2026-96951>
3. <https://windowsforum.com/news/cisa-kev-adds-exploited-windows-motw-bypass-and-ivanti-connect-secure-flaw.448188>
4. <https://www.cisa.gov/news-events/alerts/2026/10/13/cisa-adds-two-known-exploited-vulnerabilities-catalog>