مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# High-Severity Vulnerability in WinZip

Tracking #:432317104

Date:22-04-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in WinZip that allows malicious code to execute silently when users extract files from internet-downloaded archives, posing a significant security risk.

## TECHNICAL DETAILS:

A security vulnerability has been identified in WinZip, which allows attackers to bypass Windows' Mark-of-the-Web (MotW) security feature. The flaw enables malicious files extracted from downloaded archives to evade security warnings, exposing users to potential malware attacks and silent code execution.

**Vulnerability Details:**

- **CVE-2025-33028**
- CVSS v3.0 score: 7.8 (High)
- WinZip fails to propagate the MotW tag to files extracted from archives downloaded from the internet. As a result, extracted files are treated as trusted local files by Windows, bypassing security prompts and protections. Attackers can exploit this by delivering malicious archives (e.g., .zip, .7z) containing weaponized documents or executables. When a user extracts these with WinZip, the files lose the MotW tag and can execute without warning, enabling arbitrary code execution in the user's context.
- Exploitation of this vulnerability can lead to:
    - **Arbitrary Code Execution:** Attackers can execute malicious code on the victim's system.
    - **Privilege Escalation:** Malicious payloads may run with the user's privileges.
    - **Information Disclosure:** Sensitive data on the compromised system may be accessed or exfiltrated.

**Affected Products:**

- WinZip versions up to 76.9 (Windows 64-bit)
- No official fix is available at this time.

## RECOMMENDATIONS:

- **Avoid extracting untrusted archives with WinZip.**
- **Use alternative archive tools** (e.g., Windows' built-in extractor) that correctly propagate MotW tags.
- **Deploy endpoint protection** to detect and block malicious macro or script execution.
- **Educate users** about the risks of opening files from untrusted sources and the current WinZip vulnerability.
- **Monitor for updates** from WinZip and apply patches promptly once available

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:


- https://nvd.nist.gov/vuln/detail/CVE-2025-33028