مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in WinZip

Tracking #:432316556

Date:25-11-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in WinZip that could be exploited to gain unauthorized access, execute malicious code, and steal sensitive information from vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-8811**
- CVSS Score: 7.8 (High)
- A security vulnerability has been identified in WinZip, a popular file compression and archiving software. This vulnerability could potentially allow attackers to bypass security measures and execute malicious code on affected systems.
- The vulnerability exploits a flaw in WinZip's handling of the "Mark-of-the-Web" (MotW) security feature. This Windows security mechanism flags files downloaded from the internet, warning users of potential risks and triggering additional security precautions. WinZip inadvertently strips away this crucial MotW flag when processing downloaded archive files, potentially misleading users about the safety of the contents.
- Successful exploitation of this vulnerability could lead to severe consequences, including:
    - **Malware Execution:** Attackers could deliver and execute malicious software, such as ransomware, spyware, or Trojans.
    - **Data Theft:** Sensitive information could be stolen, leading to identity theft or financial loss.
    - **System Compromise:** Attackers could gain unauthorized access to the system and its resources.

Affected Versions:

- WinZip versions prior to 76.8

Fixed Versions:

- WinZip version 76.8 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-8811