مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Bypass Vulnerability in WinRAR

Tracking #:432315754

Date:05-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in WinRAR software which could allow a malicious user to bypass the authentication mechanism.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-30370,** (CVSS 4.3 MEDIUM)- RARLAB WinRAR Mark-Of-The-Web Bypass Vulnerability.
- This vulnerability allows remote attackers to bypass the Mark-Of-The-Web protection mechanism on affected installations of RARLAB WinRAR.
- User interaction is required to exploit this vulnerability in that the target must perform a specific action on a malicious page. The specific flaw exists within the archive extraction functionality.
- A crafted archive entry can cause the creation of an arbitrary file without the Mark-Of-The-Web. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current user.

Affected Versions:

- WinRAR up to version 6.24

Fixed Versions:

- WinRAR (7.0 or later)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the latest version provided by WinRAR.

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:

1. https://www.zerodayinitiative.com/advisories/ZDI-24-357/