UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 0405

## WINRAR VULNERABLE TO REMOTE CODE EXECUTION

**DATE ISSUED:** 23rd August 2023

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | **HIGH** |
| EASE OF EXPLOIT | **HARD** | MEDIUM | EASY |

## OVERVIEW

A high-severity vulnerability has been discovered in the WinRAR utility that a threat actor could potentially exploit to achieve remote code execution on Windows systems.

## BREAKDOWN

WinRAR is a popular Windows file archiver utility that millions of users use worldwide. It can easily execute commands on a computer by opening an archive. A high-severity vulnerability tracked as CVE-2023-40477 has been discovered in the WinRAR utility that originates from improper validation while processing recovery volumes. An attacker could exploit it to execute arbitrary code on the target system. However, to successfully exploit this vulnerability, a target must trick a victim into opening a specially crafted archive file. RARLAB has released the latest version of WinRAR, version 6.23, that addresses recovery volume processing code vulnerability and an issue with specially crafted archives leading to wrong file initiation.

## REMEDIATION STEPS

- Upgrade to the latest version, WinRAR version 6.23, addresses this vulnerability.
- Install and update trusted antivirus software on all your devices.
- Educate users to avoid clicking on links or attachments they receive in unsolicited emails or texts.
- Implement multi-factor authentication (MFA) to add an extra layer of security to device access.

## REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/winrar-flaw-lets-hackers-run-programs-when-you-open-rar-archives/

Help Net Security https://www.helpnetsecurity.com/2023/08/21/cve-2023-40477/

The Hacker News https://thehackernews.com/2023/08/new-winrar-vulnerability-could-allow.html