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

# CYBER GUIDANCE ISSUE 0328

## JUNE – PATCH TUESDAY

## DATE ISSUED: 15th June 2023

IMPACT: LOW | MEDIUM | **HIGH**

EASE OF EXPLOIT: HARD | **MEDIUM** | EASY

## OVERVIEW

Microsoft has addressed 78 security flaws, including 38 Remote Code Execution (RCE) vulnerabilities in the latest "Patch Tuesday" roll. Six vulnerabilities have been classified as 'Critical' for allowing Denial of Service (DoS), Remote Code Execution, and elevation of privileges attacks.

## BREAKDOWN

**Microsoft Windows:**

- 78 updates in total
- Prominent Vulnerabilities
  1. Microsoft SharePoint Server Elevation of Privilege vulnerability CVE-2023-29357 **CVSS:** 9.8
  2. Microsoft Exchange Server Remote Code Execution Vulnerability CVE-2023-32031 **CVSS:** 8.8
- Six categorised as CRITICAL
- Remote Code Execution Vulnerabilities (Excel, OneNote, and Outlook)

  CVE-2023-33133, CVE-2023-33137, CVE-2023-33140, CVE-2023-33131

**Other vendor releases:**

- Cisco
- Fortinet
- Google
- MOVEit
- VMware

## REMEDIATION STEPS

- Back up all critical data before performing updates.
- Install the latest security updates and patches – See the resources below for a complete list.

## REFERENCES & RESOURCES

| | |
|---|---|
| Microsoft | https://msrc.microsoft.com/update-guide |
| Bleeping Computer | https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2023-patch-tuesday-fixes-78-flaws-38-rce-bugs/ |
| Cisco | https://sec.cloudapps.cisco.com/security/center/publicationListing.x |
| Fortinet | https://www.fortiguard.com/psirt/FG-IR-23-097 |
| MOVEit | https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 |