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

CYBER GUIDANCE ISSUE 0315

MAY – PATCH TUESDAY

DATE ISSUED: 8th May 2023

IMPACT: LOW | MEDIUM | HIGH

EASE OF EXPLOIT: HARD | MEDIUM | EASY

OVERVIEW

Microsoft has addressed 38 CVEs in the latest "Patch Tuesday" roll, including three actively exploited zero-day vulnerabilities. Six vulnerabilities have been classified as 'Critical' for allowing remote code execution, Security feature bypass, or elevation of privileges attacks.

BREAKDOWN

Microsoft Windows:

- 38 updates in total (3 zero-day)
  1. Win32k Elevation of Privilege Vulnerability CVE-2023-29336 **CVSS:** 7.8
  2. Secure Boot Security Feature Bypass Vulnerability CVE-2023-24932 **CVSS:** 6.7
  3. Windows OLE Remote Code Execution Vulnerability CVE-2023-29325 **CVSS**: 8.1
- Six classified as CRITICAL
- Remote Code Execution Vulnerabilities

  CVE-2023-24955, CVE-2023-28283, CVE-2023-24941, CVE-2023-24943, CVE-2023-24903

Other vendor releases:

- Apple
- Cisco
- CISA
- Google
- SAP

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-may-2023-patch-tuesday-fixes-3-zero-days-38-flaws/
Apple	https://support.apple.com/en-nz/HT201222
Cisco	https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Sophos News	https://news.sophos.com/en-us/2023/05/09/mays-patch-tuesday-haul-touches-a-six-pack-of-product-families/