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

CYBER GUIDANCE ISSUE 0305

APRIL – PATCH TUESDAY

DATE ISSUED: 17th April 2023

IMPACT: LOW | MEDIUM | **HIGH**

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

OVERVIEW

Microsoft has addressed 97 CVEs in the latest "Patch Tuesday" roll, including one actively exploited zero-day vulnerability. Seven vulnerabilities have been classified as 'Critical' for allowing remote code execution, Security feature bypass, or elevation of privileges attacks.

BREAKDOWN

Microsoft Windows:

- 97 updates in total (1 zero-day)
  Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE-2023-28252 **CVSS:** 7.8
- 7 classified as CRITICAL
- Remote Code Execution Vulnerabilities
  CVE-2023-28285, CVE-2023-28295, CVE-2023-28287, and CVE-2023-28311.

Other vendor releases:

- Apple
- Cisco
- Fortinet
- Google

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
Bitdefender	https://www.bitdefender.com/blog/hotforsecurity/apple-patches-first-zero-day-flaw-reported-in-2023-on-ios-and-macos/
Bleeping Computer	https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2023-patch-tuesday-fixes-1-zero-day-97-flaws/
Cisco	https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Sophos News	https://news.sophos.com/en-us/2023/04/11/april-showers-windows-updates-on-sysadmins/