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

CYBER GUIDANCE ISSUE 00278

FEBRUARY - PATCH TUESDAY

DATE ISSUED: 14th February 2023

IMPACT: LOW | MEDIUM | HIGH

EASE OF EXPLOIT: HARD | MEDIUM | EASY

OVERVIEW

77 CVE's have been addressed by Microsoft in the latest "Patch Tuesday" roll out which includes three actively exploited zero-day vulnerabilities. A vulnerability is classified as a zero day-day vulnerability if it is publicly disclosed or actively exploited without a security patch available.

BREAKDOWN

Microsoft Windows:

- 77 updates in total (3 zero-days)
  Windows Graphics Component Remote Code Execution CVE-2023-21823 **CVSS:** 7.8
  Microsoft Publisher Security Features Bypass Vulnerability CVE-2023-21715 **CVSS:** 7.3
  Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE-2023-23376 **CVSS:** 7.8
- 9 classified as CRITICAL (all RCE)

Other vendor releases:

- Adobe
- Atlassian
- Fortra
- Apple
  Zero-Day CVE-2023-23529

REMEDIATION STEPS

- Back up all critical data before performing updates.
- Install latest security updates and patches – For a full list see the resources listed below.

REFERENCES & RESOURCES

Microsoft	https://msrc.microsoft.com/update-guide
Apple	https://support.apple.com/en-us/HT213635
Bleeping Computer	https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/
Security Week	https://www.securityweek.com/adobe-plugs-critical-security-holes-in-illustrator-after-effects-software/
Atlassian	https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-2023-02-01-1188786458.html
Bleeping Computer	https://www.bleepingcomputer.com/news/security/actively-exploited-goanywhere-mft-zero-day-gets-emergency-patch/