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

# CYBER GUIDANCE ISSUE 00291

## MARCH - PATCH TUESDAY

## DATE ISSUED: 20th March 2023

IMPACT: LOW | MEDIUM | HIGH

EASE OF EXPLOIT: HARD | MEDIUM | EASY

## OVERVIEW

83 CVE's have been addressed by Microsoft in the latest "Patch Tuesday" roll out which includes two actively exploited zero-day vulnerabilities. Nine vulnerabilities have been classified as 'Critical' for allowing remote code execution, denial of service, or elevation of privileges attacks.

## BREAKDOWN

**Microsoft Windows:**

- 83 updates in total (2 zero-days)
  Microsoft Outlook Elevation of Privilege Vulnerability
  CVE-2023-23397 **CVSS:** 9.8
  Windows SmartScreen Security Feature Bypass Vulnerability
  CVE-2023-24880 **CVSS:** 5.4
- 9 classified as CRITICAL

**Other vendor releases:**

- Apple
- Atlassian
- Cisco
- Fortinet
- Google

## 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/HT213650 |
| Bleeping Computer | https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2023-patch-tuesday-fixes-2-zero-days-83-flaws/ |
| Cisco | https://sec.cloudapps.cisco.com/security/center/publicationListing.x |
| Sophos News | https://news.sophos.com/en-us/2023/03/14/march-2023-patch-tuesday/ |