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

CYBER GUIDANCE ISSUE 0402

AUGUST – PATCH TUESDAY

DATE ISSUED: 16th June 2023

IMPACT: LOW | MEDIUM | **HIGH**

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

OVERVIEW

Microsoft has addressed 87 security flaws, including 23 Remote Code Execution (RCE) vulnerabilities in the latest "Patch Tuesday" roll. Two zero-day vulnerabilities are included in the patch. Six vulnerabilities have been classified as 'Critical' for allowing Denial of Service (DoS), Remote Code Execution, and elevation of privileges attacks.

BREAKDOWN

Microsoft Windows:

- 87 updates in total
- Zero-day vulnerabilities
  1. ADV2300 - Microsoft Office Defense in Depth Update CVE-2023-36884 **CVSS:** 8.8
  2. .NET and Visual Studio Denial of Service Vulnerability CVE-2023-38180 **CVSS**: 7.5
- Six categorised as CRITICAL
- Remote Code Execution Vulnerabilities (.NET, Microsoft Message Queuing, Microsoft Teams, Microsoft Outlook)
  CVE-2023-36895 CVE-2023-29328 CVE-2023-29330 CVE-2023-35385 CVE-2023-36911 CVE-2023-36910

Other vendor releases:

- Adobe
- AMD
- Google
- Ivanti
- MOVEit
- PaperCut

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-august-2023-patch-tuesday-warns-of-2-zero-days-87-flaws/
Adobe	https://helpx.adobe.com/security.html
Google	https://source.android.com/docs/security/bulletin/2023-08-01