

CYBER GUIDANCE ISSUE 00237

JANUARY - PATCH TUESDAY

DATE ISSUED: 18th January 2022

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

97 Vulnerabilities are addresses in the first Microsoft Patch Tuesday for 2022 including 9 CVE’s with a critical rating, one receiving a 9.8 for a wormable bug and two zero-days under know active exploit in the wild.

Products receiving updates includes Windows & Windows components, Chromium-based Edge Browser, Exchange Server, Office & Office components, SharePoint Server, .NET framework, Dynamics, Open-Source Software, Hyper-V Hypervisor, Defender and Remote Desktop Protocol (RDP).

BREAKDOWN

Microsoft Windows:

- 97 updates in total (6 zero-days)
- 9 rated CRITICAL
 - CVE-2022-21907 9.8 CVSS Wormable Bug
 - CVE-2022-21919 & CVE-2022-21836 under active exploit
 - CVE-2021-22947, CVE-2021-36976, CVE-2022-21874, CVE-2022-21839, CVE-2022-21840, CVE-2022-21833, CVE-2022-21912, CVE-2022-21898, CVE-21917
- 87 rated IMPORTANT
- 1 rated MODERATE

Other vendor releases:

- Google Chrome
- Mozilla
- Apple
- Adobe
- Android
- SAP
- Cisco
- VMWare

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
	https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan
Bleeping Computer	https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2022-patch-tuesday-fixes-6-zero-days-97-flaws/
Threatpost	https://threatpost.com/microsoft-wormable-critical-rce-bug-zero-day/177564/