Patch Tuesday: Microsoft Warns of Exploited Windows Zero-Days

Microsoft’s Patch Tuesday machine is humming loudly with software updates to fix at least 76 vulnerabilities in Windows and OS components and the company is warning that some of the bugs have already been exploited in the wild.

Microsoft’s security response team flagged three of the 76 documented flaws in the already-exploited category that typically refers to zero-day malware attacks in the wild.

As is customary, the world’s largest software maker did not provide any technical details of the exploited vulnerabilities or IOCs (indicators of compromise) to help defenders hunt for signs of compromise.

The most serious of the exploited issues is documented as CVE-2023-21823, a Windows graphics component remote code execution vulnerability. “An attacker who successfully exploited this vulnerability could gain SYSTEM privileges,” according to a barebones advisory from Redmond that credits researchers at incident response giant Mandiant with reporting the issue.

The company also called special attention to CVE-2023-21715, a feature bypass vulnerability in Microsoft Publisher that’s in the already-exploited category; and CVE-2023-23376, a privilege escalation flaw in Windows common log file system driver.

Microsoft slapped critical-severity ratings on seven of the 76

bulletins and warned that these issues could lead to remote code execution attacks targeting Microsoft Word, Visual Studio and the Windows iSCSI Discovery Service.

The company also shipped important-severity updates for Microsoft Defender, Microsoft Exchange Server, Microsoft Dynamics, 3D Builder, Sharepoint and Microsoft SQL Server.

The industry-wide Patch Tuesday updates also included security fixes from Adobe (critical bugs in After Effects and Illustrator) and Apple (WebKit zero-day exploitation on iOS and macOS).

According to Adobe's security bulletins, the Illustrator and After Effects patches carry critical-severity ratings because of the risk of code execution attacks.

The WebKit flaw, tracked as CVE-2023-23529, is a type confusion issue that can be exploited for arbitrary code execution by getting the targeted user to access a malicious website. Apple marked this as exploited on its flagship iOS mobile platform.

Related: Apple Patches Actively Exploited WebKit Zero-Day Vulnerability

Related: Microsoft Patch Tuesday: 97 Windows Vulns, 1 Exploited Zero-Day

Related: Zoom Patches High Risk Flaws on Windows, MacOS Platforms

Related: Microsoft Warns of Under-Attack Windows Kernel Flaw

Patch Tuesday: Microsoft Warns of Exploited Windows Zero-Days