Microsoft Patches Another Already-Exploited Windows Zero-Day

For the second month in a row, Microsoft is pushing out urgent patches to cover an already-exploited vulnerability in its flagship Windows operating system.

The vulnerability, flagged as zero-day by researchers at Mandiant, is described as an elevation of privilege issue in the Windows Common Log File System driver.

In an advisory documenting the CVE-2023-28252, Redmond warns that an attacker who successfully exploited this vulnerability could gain SYSTEM privileges.

As is customary, Microsoft did not provide any additional details on the zero-day exploitation or release IOCs (indicators of compromise) to help defenders hunt for signs of infections.

The latest zero-day warning headlines a busy Patch Tuesday that includes fixes for at least 98 documented vulnerabilities across the Windows ecosystem. It comes exactly a month after Redmond confirmed a major no-interaction Outlook vulnerability exploited by Russian hackers since at least April 2022.

So far this year, there have been at least 19 in-the-wild zero-day attacks. Security defects in code from Microsoft feature in about one-third of all observed exploitation in 2023.

According to ZDI, organizers of the Pwn2Own exploit contest, none of the bugs disclosed over Teams during Pwn2Own Vancouver

are being addressed by Microsoft this month.

In a blog post, ZDI also recommends that Windows users pay attention to CVE-2023-21554, a Microsoft Message Queuing remote code execution vulnerability with a CVSS score of 9.8 out of 10.

“[This bug] allows a remote, unauthenticated attacker to run their code with elevated privileges on affected servers with the Message Queuing service enabled. This service is disabled by default but is commonly used by many contact center applications,” ZDI said.

The Microsoft patches come on the same day Adobe rolled out security fixes for at least 56 vulnerabilities in a wide range of products, some serious enough to expose Windows and macOS users to code execution attacks.

Adobe called special attention to its APSB23-24 bulletin that covers critical-severity security flaws in the widely deployed Adobe Acrobat and Reader software.

“Successful exploitation could lead to arbitrary code execution, privilege escalation, security feature bypass and memory leak,” Adobe said in a warning addressed to both Windows and macOS users.

The company documented at least 16 vulnerabilities in the Acrobat and Reader updates and said it was not aware of any in-the-wild exploitation.

Related: Apple Ships Urgent iOS Patch for Newly Exploited Zero-Days

Related: Adobe Plugs Gaping Security Holes in Reader, Acrobat

Related: Samsung Mobile Chipsets Vulnerable to Baseband Code Execution Exploits

Related: Microsoft: No-Interaction Outlook Zero Day Exploited

Since Last April

Microsoft Patches Another Already-Exploited Windows Zero-Day