Windows Zero-Day Exploited in Nokoyawa Ransomware Attacks

A Windows zero-day vulnerability fixed by Microsoft with its April 2023 Patch Tuesday updates has been exploited by cybercriminals in ransomware attacks, according to Kaspersky.

Microsoft's latest round of security updates addresses roughly 100 vulnerabilities, including CVE-2023-28252, which has been described as a privilege escalation flaw affecting the Windows Common Log File System (CLFS) driver.

Microsoft warned that the vulnerability has been exploited in the wild, but did not share any information on the attacks.

Kaspersky, Mandiant and Chinese cybersecurity firm DBAppSecurity have been credited for reporting CVE-2023-28252, and Kaspersky on Tuesday shared some details about the attacks exploiting the vulnerability.

CLFS is a log file subsystem described by Microsoft as a general-purpose logging service that can be used by software clients running in user- or kernel-mode. The vulnerability affecting CLFS allows an authenticated attacker to elevate privileges to System.

According to Kaspersky, a cybercrime group known for conducting ransomware operations has been exploiting the vulnerability as part of attacks whose goal is to deliver the Nokoyawa ransomware.

"This group is notable for its use of a large number of similar but unique Common Log File System (CLFS) driver exploits that were likely developed by the same exploit author. Since at least June 2022, we've identified five

different exploits used in attacks on retail & wholesale, energy, manufacturing, healthcare, software development and other industries," Kaspersky noted.

The Nokoyawa ransomware family, which is designed to target Windows systems, emerged in February 2022. The malware encrypts files on compromised systems, but the cybercriminals also claim to steal valuable information that they threaten to leak unless a ransom is paid.

Code similarities suggest ties to the Karma and Nemty ransomware families, while attack chain similarities connect it to the notorious Hive operation, disrupted recently by law enforcement.

Kaspersky has not shared too many details on the vulnerability in an effort to prevent abuse. The company plans on releasing additional information nine days after Patch Tuesday.

Kaspersky pointed out that dozens of CLFS vulnerabilities were discovered in the past five years and at least three of them – not including CVE-2023-28252 – have been exploited in the wild.

Related: Veritas Vulnerabilities Exploited in Ransomware Attacks Added to CISA 'Must Patch' List

Related: Patch Tuesday: Microsoft Warns of Exploited Windows Zero-Days

Related: Microsoft Pins Outlook Zero-Day Attacks on Russian Actor, Offers Detection Script

Windows Zero-Day Exploited in Nokoyawa Ransomware Attacks