BLACKSWAN
CYBERSECURITY

THREAT ANALYSIS
April 13, 2023

Windows Zero-Day Vulnerability (CVE-2023-28252) Exploited in Ransomware Attacks

SUMMARY

A zero-day vulnerability in the Windows Common Log File System (CLFS) is actively being exploited by cybercriminals to escalate privileges and deploy the Nokoyawa ransomware. CISA added CVE-2023-28252 (CVSSv3 Score is 7.8) to its catalog of Known Exploited Vulnerabilities ordering agencies to secure their systems by May 2nd.

Microsoft has published a patch for this zero-day and 96 other security bugs as part of April's Patch Tuesday, including 45 remote code execution vulnerabilities.

VULNERABILITY DETAILS

The CLFS driver contains an unspecified vulnerability that allows for privilege escalation. The CLFS is a general-purpose logging service that can be used by software clients running in user-mode or kernel-mode.

The flaw can be exploited by local attackers in low-complexity attacks without user interaction. Successful exploitation enables threat actors to gain SYSTEM privileges and fully compromise targeted Windows systems (Windows Server and Windows Client versions).

ATTACK METHODS

In February 2023, Kaspersky's Global Research and Analysis Team (GReAT) found a flaw being exploited during Nokoyawa ransomware attacks.

During Kaspersky's analysis of a number of attempts to execute similar elevation of privilege exploits on Microsoft Windows servers at various small and medium-sized businesses in the Middle Eastern and North American regions found that the Nokoyawa ransomware gang used various exploits to target the Common Log File System (CLFS) driver. These attacks were seen as far back as June 2022, with similar characteristics linking them to a single exploit developer.

Target industries include energy, healthcare, manufacturing, retail, and software development.

Exploitation Artifacts

- C:\Users\Public\.container*
- C:\Users\Public\MyLog*.blf
- C:\Users\Public\p_* Exploit
- 46168ed7dbe33ffc4179974f8bf401aa

CobaltStrike Loaders

- 1e4dd35b16ddc59c1ecf240c22b8a4c4
- f23be19024fcc7c8f885dfa16634e6e7
- a2313d7fdb2f8f5e5c1962e22b504a17

CobaltStrike C2s

- vnssinc[.]com
- qooqle[.]top
- vsexec[.]com
- devsetgroup[.]com

Nokoyawa Ransomware

- 8800e6f1501f69a0a04ce709e9fa251c

REFERENCES

- Apply Windows security updates.
- Employ behavior-based / behavior-analytic detection capabilities to automatically detect and prevent malware early in the attack chain to prevent its execution.