CVE-2023-28252 Summary:
Vulnerability Type: Privilege Escalation
Target Component: Common Log File System (CLFS)
Risk Level: Critical
Exploitation Date: February 2022 onwards
Patch Released by Microsoft: April 2023

Background:
The Nokoyawa ransomware group has been active since February 2022, and it was only in April 2023 that Microsoft released a patch to address this issue. This vulnerability has been used as a means for attackers to gain unauthorized access to Windows systems, making it imperative for us to apply the necessary patch to safeguard our infrastructure.
According to Kaspersky's analysis, the Nokoyawa ransomware group has used other exploits targeting the CLFS driver since June 2022, with similar but distinct characteristics, all linked to a single exploit developer.

Actions Required:
Immediate Patching: We strongly recommend applying the security patch released by Microsoft for CVE-2023-28252 as soon as possible to mitigate the risk associated with this vulnerability. Failing to do so could leave our servers exposed to potential exploitation.

Review and Monitoring: In addition to patching, we should conduct a thorough review of our server logs to check for any signs of suspicious activity or unauthorized access. Continuous monitoring of our server environment is crucial to ensure the security of our systems.

Security Awareness: It is essential to remind all team members of the importance of practicing good cybersecurity hygiene. Encourage the use of strong, unique passwords and two-factor authentication wherever applicable.

Incident Response Plan: Ensure that our incident response plan is up-to-date and ready for immediate activation in case of any security incidents. Timely detection and response are critical in mitigating the impact of potential attacks.