AL2024_31 Windows Driver Zero-Day Exploited by Lazarus Hackers to Install Rootkit (August 20th , 2024)

Description

The notorious Lazarus hacking group, attributed to North Korea, has exploited a zero-day vulnerability in the Windows Ancillary Function Driver for WinSock (AFD.sys), a critical system component, to elevate privileges and install the FUDModule rootkit on targeted systems. This flaw, identified as **CVE-2024-38193**, was disclosed and patched by Microsoft during their August 2024 Patch Tuesday, along with seven other zero-day vulnerabilities.

Attack Details

The CVE-2024-38193 vulnerability is a Bring Your Own Vulnerable Driver (BYOVD) attack vector, where the attackers exploited the AFD.sys driver to gain kernel-level privileges. The AFD.sys driver, which is installed by default on all Windows devices, acts as an entry point into the Windows Kernel for the Winsock protocol. By leveraging this vulnerability, the Lazarus group was able to bypass Windows monitoring features and evade detection by installing the FUDModule rootkit.

Remediation

To mitigate the risks associated with **CVE-2024-38193**, it is crucial to apply the security updates released by Microsoft in August 2024 immediately. These updates address the vulnerability in the AFD.sys driver, preventing the exploitation vector used by the Lazarus group.

1. **Monitor for Abnormal Behavior:** Implement monitoring for unusual activity associated with the AFD.sys driver and kernel-level processes.
2. **Enhance Endpoint Protection:** Deploy robust endpoint protection solutions that can detect and block the installation of unauthorized drivers and rootkits.
3. **Review and Harden Security Configurations:** Ensure that systems are configured to block known vulnerable drivers and that security policies are regularly reviewed and updated.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

Specops Software. (2024, August 14). *Are you blocking "keyboard walk" passwords in your Active Directory?* Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/are-you-blocking-keyboard-walk-passwords-in-your-active-directory/

Zorz, Z. (2024, August 20). *0-day in Windows driver exploited by North Korean hackers to deliver rootkit (CVE-2024-38193) - Help Net Security*. Retrieved from Help Net Security. https://www.helpnetsecurity.com/2024/08/20/0-day-in-windows-driver-exploited-by-north-korean-hackers-to-deliver-rootkit-cve-2024-38193/