BLACKSWAN CYBERSECURITY

THREAT ADVISORY

August 28, 2024

Lazarus Group Exploits Windows Driver Zero-Day to Deploy Rootkit

SUMMARY

The Lazarus hacking group exploited a zero-day vulnerability in the Windows AFD.sys driver (CVE-2024-38193) to elevate privileges and install the FUDModule rootkit. This vulnerability, patched in August 2024, allowed attackers to evade detection by disabling Windows monitoring features. The flaw was used in a targeted campaign, potentially linked to attacks on Brazilian cryptocurrency professionals.

TECHNICAL DETAILS

The Lazarus hacking group is infamous for large-scale cyberheists targeting financial and cryptocurrency firms to fund North Korea's weapons programs. In 2022, the US linked them to a $617 million cryptocurrency theft from Axie Infinity and offers up to $5 million for information on their activities.

The notorious North Korean Lazarus hacking group leveraged the zero-day flaw in the Windows Ancillary Function Driver for WinSock (AFD.sys), identified as CVE-2024-38193, to execute a Bring Your Own Vulnerable Driver (BYOVD) attack. This vulnerability allowed them to gain kernel-level privileges, enabling the installation of the FUDModule rootkit, which is designed to evade detection by disabling Windows monitoring mechanisms. The AFD.sys driver, a default component on all Windows devices, made this attack particularly dangerous, as it required no additional vulnerable drivers that could be easily blocked or detected by Windows.

The attack was uncovered by Gen Digital researchers in June 2024 and is believed to be connected to a larger campaign in Brazil, where North Korean hackers, identified as PUKCHONG (UNC4899), targeted cryptocurrency professionals. The attackers used social engineering tactics, including fake job opportunities, to deliver a trojanized Python application that ultimately led to the installation of malware.

The AFD.sys vulnerability was one of several zero-day flaws patched by Microsoft in August 2024. The Lazarus group has a history of exploiting similar vulnerabilities, including the Windows appid.sys and Dell dbutil_2_3.sys kernel drivers, to install the FUDModule rootkit in previous BYOVD attacks.

INDICATORS OF COMPROMISE (IOCs)

AVAST's IOC Github has a YARA module - ioc/FudModule at master · avast/ioc · GitHub

RECOMMENDATIONS

- Ensure all systems are updated with the latest security patches, including the August 2024 Patch Tuesday update.
- Implement advanced monitoring solutions to detect unusual behavior related to drivers and kernel-level activities.
- Maintain strict control over driver installations, allowing only trusted and verified drivers.
- Employ endpoint protection solutions that can block the execution of known vulnerable drivers.
- Utilize application whitelisting to prevent unapproved executables, including vulnerable drivers, from running.
- Segment networks to limit the impact of any potential breaches, reducing the attack surface available to threat actors.
- Conduct regular security awareness training to ensure employees are aware of the latest phishing and social engineering tactics used by groups like Lazarus.

REFERENCES

- https://thehackernews.com/2024/08/microsoft-patches-zero-day-flaw.html
- https://www.bleepingcomputer.com/news/microsoft/windows-driver-zero-day-exploited-by-lazarus-hackers-to-install-rootkit/
- https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/
- https://www.rapid7.com/db/vulnerabilities/msft-cve-2024-38193/