Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 240 **05-03-2024**

Name: Lazarus Group Exploits Windows Kernel Zero-Day for Privilege Escalation

Threat Classification: Zero-Day Exploitation

Affected Software / Services:

- Windows 10, version 1703 (RS2/15063) and potentially other versions using the vulnerable IOCTL handler.

Summary:

The Lazarus Group, a notorious hacking entity, utilized a recently patched privilege escalation flaw (CVE-2024-21338) in the Windows Kernel as a zero-day. This exploit granted the attackers kernel-level access, enabling them to disable security software on compromised systems. The vulnerability, initially introduced in Windows 10, version 1703, could allow an attacker to gain SYSTEM privileges by running a specially crafted application after logging into the system. Lazarus Group's exploit went beyond typical Bring Your Own Vulnerable Driver (BYOVD) attacks, utilizing a zero-day in the appid.sys driver, a component crucial to AppLocker, to execute arbitrary code and deploy their sophisticated FudModule rootkit.

Severity	**Critical**
Attack Vector	Zero-Day Kernel Exploit

Recommendations:

- Ensure all Windows operating systems are promptly updated with the latest security patches to mitigate the CVE-2024-21338 vulnerability.
- Implement continuous monitoring for any signs of the Lazarus Group's FudModule rootkit, especially in the context of system loggers and security software.
- Given the Lazarus Group's sophisticated tactics, enhance security measures to detect and prevent kernel-level exploits, including monitoring for unusual code execution and kernel object manipulation.
- Educate users on recognizing and avoiding potential attack vectors, emphasizing the importance of not executing untrusted or suspicious applications.
- Employ network segmentation strategies to limit the lateral movement of attackers within the network, reducing the potential impact of a successful compromise.
- Work closely with cybersecurity vendors to stay updated on evolving threats, IoCs, and detection strategies related to Lazarus Group activities.
- Reinforce endpoint protection mechanisms to identify and block malicious activities associated with Lazarus Group tools, including FudModule.
- In case of any incident, please report to this office, through PTA CERT Portal and email.