Microsoft Outlook Zero-Day Exploited in the Wild

Microsoft disclosed a new zero-day vulnerability in Outlook identified as CVE-2023-23397. This flaw is an elevation-of-privilege (EoP) vulnerability that enables remote code execution capability as threat actors can steal NTLM credentials of Microsoft Outlook users. Threat actors send a specially crafted email containing a malicious calendar or meeting invite with a custom notification sound that bypasses the default Waveform (WAV) file. This notification acts as a path to a Server Message Block (SMB) that enables shared control for the threat actor. The email automatically triggers the flaw once it makes it to the user's inbox. No interaction with the victim is required for this vulnerability to be exploited. All supported versions of Microsoft Outlook for Windows are affected; however, web-based Microsoft 365 is not vulnerable because Windows New Technology LAN Manager (NTLM) authentication is not supported.

Microsoft revealed that a Russian-based threat actor was identified using this vulnerability to target several organizations in government, transportation, energy, and military sectors in Europe over the past year. While Microsoft did not disclose the hacking group, they did link the group to Russian military intelligence. This flaw poses a significant risk to organizations as threat actors can repeatedly execute this attack to gain access/control of a victim's systems.

Microsoft recommends companies organizations block outbound SMB port 445 traffic preventing NTLM authentication messages from being sent to remote file shares and adding users to the Protected Users security group restricting NTLM from being used as an authentication method.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.darkreading.com/threat-intelligence/emotet-resurfaces-yet-again-after-three-month-hiatus
2. https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/
3. https://www.bleepingcomputer.com/news/security/emotet-malware-attacks-return-after-three-month-break/
4. https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html