Four Windows vulnerabilities can be exploited in the perfect attack chain

The vulnerabilities include: 2 remote code execution errors, 1 privilege escalation error and 1 Secure Boot security feature bypass error. Under ideal conditions, hackers can combine 4 vulnerabilities to form a perfect attack chain.

According to Bkav's cybersecurity experts, the first vulnerability (identification code CVE-2023-29325) is a remote code execution error in OLE (Object Linking & Embedding) technology on Windows, affecting Outlook.

To exploit, a hacker sends a malicious phishing email to the user. As long as the victim opens the email using Outlook software, or the Outlook application displays a preview of the email, the attacker can remotely execute code and take complete control of the device.

The second vulnerability, CVE-2023-29336, is an escalation of privilege error in the operating system's Win32k kernel driver. Successfully exploited, hackers can escalate from user to SYSTEM privilege (the highest privilege in the operating system), thereby installing malicious code on the target device and maintaining access. The vulnerability is currently being exploited in real attacks.

The third vulnerability, CVE-2023-24932, allows hackers to bypass the Secure Boot secure boot feature. To exploit, hackers seek to 'hide' or gain administrative rights on the target device, thereby installing bootkit malware on the system firmware. This bootkit allows hackers to take control of the device boot process, stay hidden longer and avoid detection by security solutions.

The most dangerous is the remote code execution vulnerability CVE-2023-24941 (CVSS severity score 9.8/10), which can be a springboard for hackers to deeply attack other systems. The vulnerability exists in the file sharing protocol in Windows' NFS (Network File System) network.

An unauthenticated attacker could send a specially crafted command to the NFS service, thereby gaining control of Windows servers. CVE-2023-24941 affects Windows Server 2012, 2016, 2019, and 2022 and specifically does not require user interaction.

According to Bkav experts, under ideal conditions, hackers can combine the above 4 vulnerabilities to form an attack chain as follows:

First, trick the victim into clicking on a fake email to exploit CVE-2023-29325, thereby gaining remote code execution on the target device.

Next, privilege escalation from user level to system privileges via CVE-2023-29336, which then infects the device with malware and maintains access.

Once on the device, hackers can exploit the Secure Boot security feature with CVE-2023-24932, install malware and maintain presence on the victim's system.

Finally, taking advantage of CVE-2023-24941 to exploit deeply into Windows servers.

> 'Successfully performing the attack steps, hackers can control the entire system, steal sensitive information.

In particular, the vulnerability CVE-2023-29325 puts users at risk of becoming victims of email phishing campaigns. Attacks in this form are quite easy, low cost and can be carried out on a large scale, so the impact will be huge.

It is recommended that users immediately update the Windows operating system to the latest version, the patch can be downloaded here. At the same time, users should not open strange emails of unknown origin. If abnormalities are detected on the system, they should contact the professional team to review and handle.

Microsoft fixed these errors in the May patch (Patch Tuesday).

You finished reading the article "**Four Windows vulnerabilities can be exploited in the perfect attack chain**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com