It’s a Bad Week to be Microsoft (or Last Couple of Years?)

Microsoft

Posted by Mike Heumann, March 17, 2023

We all have become accustomed to Microsoft’s “Patch Tuesdays”, where the weekly batch of bugfixes are put out. This week, Microsoft released some big ones, releasing fixes for over 80 windows security flaws. One of the most pronounced flaws addressed in this release was CVE-2023-23397, an already-exploited critical defect in Microsoft Outlook. According to a variety of sources, this security flaw allows specially-crafted emails to exploit user credentials from Outlook (specifically the Net-NTLMv2 hash), allowing the attackers to log onto an Exchange Server as the exploited user. Most interestingly, this bug can do as soon as the email hits the Outlook client, before the user opens the sees it in the Preview Pane. As usual, Microsoft’s security response center provided only the barest details on this bug, with no indicators of compromise (IOC) information that would allow defenders to identify infected machines.

Also of interest was the CVE-2023-24880 exploit that Microsoft identified this Tuesday. This exploit allows attackers to actively bypass Microsoft’s SmartScreen feature. SmartScreen, which is an extension of Microsoft Defender for the Microsoft Edge Web Browser, was intended to stop web-based phishing attacks (including downloaded malicious code). However, SmartScreen has turned into vector for malware – this is the second exploit to take advantage of its’s weaknesses (CVE-2022-44698 was the first one). The specific attack methodology that the CVE utilizes is bypassing of the Mark-of-the-Web (MOTW) security feature, which forces web pages to execute in security zone, which has been extended to other internet payloads such as files. Once MOTW is bypassed in SmartScreen, malicious payloads such as ransomware can be delivered through the unopened email. The The primary use of CVE-2023-24880 is to deliver the Magniber ransomware package, and it is believed that this weakness has been utilized to deliver roughly 1,000 malware packages to targets in the European Union.

Both of these exploits are indicative of a larger problem – that of “narrow” patches that enable attackers to build slight variants of the original exploit to get around the patches. While these narrow patches have the advantage of being able be developed and tested quickly, they do allow new exploits to be created just as quickly, as evidenced by CVE-2023-24880 (itself a variant of CVE-2022-44698).

Bret Arsenault, Chief Information Security Officer (CISO) at Microsoft likes to say, “Hackers don’t break in, they log in.”

A final issue identified was the increasing use of Microsoft OneNote to promulgate malware. Unlike the Microsoft Edge example above, OneNote does not utilize the MOTW indicator, making OneNote a great carrier for malicious payloads. While Microsoft silently patched this OneNote issue in January, the patch is not perfect. As a result, OneNote is quickly becoming a method of choice for the delivery of infected payloads, including remote access trojans (RATs), form stealers, and other credential stealers such as Quakbot/Qbot/Pinkslipbot. The only effective mitigation strategy relies on users to not open attachments that are from unknown sources.

Actually, 2021 and 2022 were also bad years (if not worse years) for Microsoft. Some of the more notable exploits during those two years include:

- March 2021: Exchange server vulnerability CVE-2021-26855
- June 2021: Six serious zero-day exploits patched (CVE-2021-33742, CVE-2021-31955, CVE-2021-31956, CVE-2021-33739, CVE-2021-31201, CVE-2021-31199)
- July 2021: PrintNightmare vulnerability (CVE-2021-34527)
- August 2021: Exchange Autodiscover vulnerability (credentials leakage); Microsoft Azure database service unrestricted access flaw
- September 2021 (a REALLY bad month): MSHTML vulnerability (CVE-2021-40444); disclosure of several “non-exploited” vulnerabilities (CVE-2021-36968, CVE-2021-38647, CVE-2021-36965, CVE-2021-36952, CVE-2021-38667, CVE-2021-36975, CVE-2021-38639); APT exploitation of ManageEngine Component of Active Directory (CVE-2021-40539); APT29/CozyBear targeting of Microsoft AD Federation Services
- January 2022: Exchange Server remote execution vulnerability (CVE-2022-21846)
- February 2022: SharePoint vulnerability (CVE-2022-22005)
- March 2022: HEVC Video Extensions remote code execution (CVE-2022-22006)
- April 2022: PrintNightmare local privilege escalation (CVE-2022-26796)
- May 2022: Windows NFS remote code execution (CVE-2022-24491/CVE-2022-24497)
- June 2022: LSA Spoofing Vulnerability (CVE-2022-26925); Internet Explorer component reuse vulnerabilities.
- July 2022: More zero-day vulnerabilities (CVE-2022-22047)
- August 2022: More Exchange Server vulnerabilities (CVE-2022-21980/CVE-2022-24516/CVE-2022-24477)
- September 2022: Windows TCP/IP remote code execution (CVE-2022-34718)
- October 2022: Workaround guidance for actively exploited Exchange Server vulnerabilities (CVE-2022-41033)

- November 2022: Exchange server patches; print spooler update (CVE-2022-41073); out-of-band Kerberos authentication issues

I have always been a used Microsoft products (since early MS-DOS in 1985!), but for a company with over $200B in revenue, and more than 100,000 software engineers as of July 2021, this is an awful security record. Seems like all of us that are Microsoft subscribers are paying Microsoft to be (at best) beta testers….Ah, I could implement Microsoft Defender!