HTTP Stack Remote Code Execution Vulnerability (CVE-2022-21907)

Submitted by Semih TURAN

Overview

A vulnerability, numbered CVE-2022-21907, has been identified targeting Microsoft operating systems. Although this vulnerability uses HTTP protocol stacks to launch an attack, it is known that this vulnerability can be exploited by sending specially crafted packets for these stacks. In this case, we know that all software without http.sys patch is vulnerable. To fix this vulnerability, we must apply the security patch that Microsoft has officially released to our systems as soon as possible.

Vulnerability

On January 12, 2022, we discovered that Microsoft Tuesday updates fixed a vulnerability in the ability to execute remote code over the Http protocol stack. There is a boundary error in the HTTP Trailer Support feature in the HTTP Stack which is causing buffer overflow. Thanks to this vulnerability, an unauthenticated attacker may execute any code on a target system via specially crafted HTTP packets to a web server. In addition, by crashing the operating system, the vulnerability might cause a denial of service condition on the victim's machine. In this case, A Proof Of Concept (PoC) has already been made public, demonstrating how this vulnerability may be exploited to cause the machine to crash (Windows Blue Screen of Death).

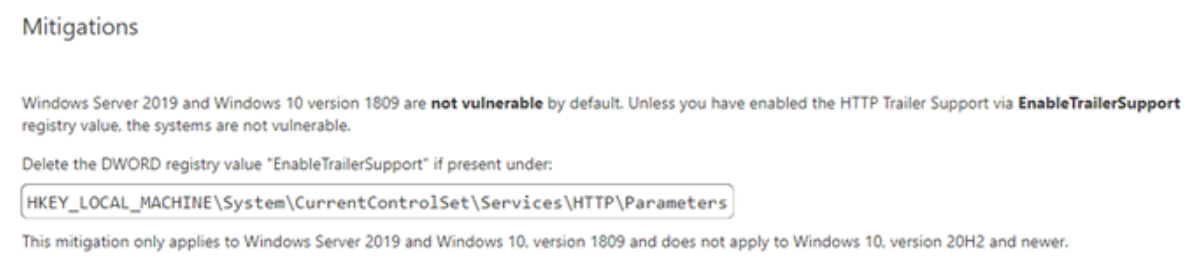

Figure 1: Microsoft website refers that vulnerability is related to HTTP Trailers

Windows devices will restart in case of a single iteration attack. After that, the function of the operating system is normal. But if there is a continuous attack, the operating system could lead to Denial of Service (DoS) conditions. In addition, unauthenticated attackers can use remote execute code so they can reach the privileges operation system.

Un-patched and Patched Version Differences

To understand Vulnerability, we need to discover the difference between two machines that do and do not receive the update patch. For this reason, we can perform difference analysis with tools such as IDO pro, BindDiff. We can see the differences in the function names in the patch binary. We can observe that there is a 10 percent difference in the function named UIFastSendHttpResponse. In addition, there was a 1 percent difference in the function named UlpAllocateFastTracker.

In UlpAllocateFastTracker, we can see the differences:

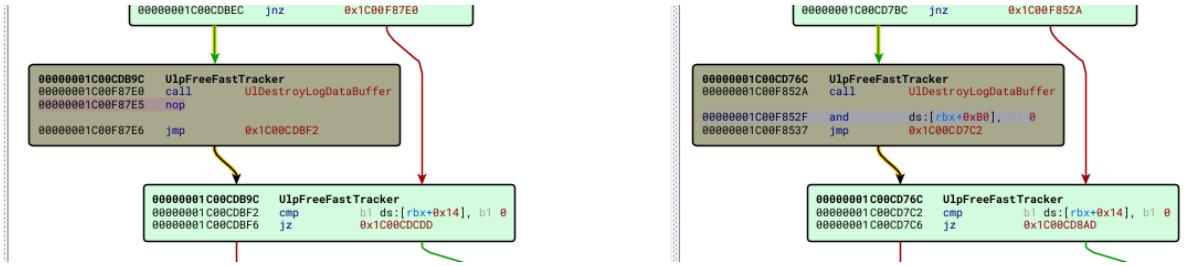

Figure 2: UlpAllocateFastTracker unpatched vs. patched version

As seen in Figure 2, UlDestroyLogDataBuffer jumps to the next block without doing anything to the unpatched version. But in the patched version, [rbx+0xb0] with AND takes the value 0.

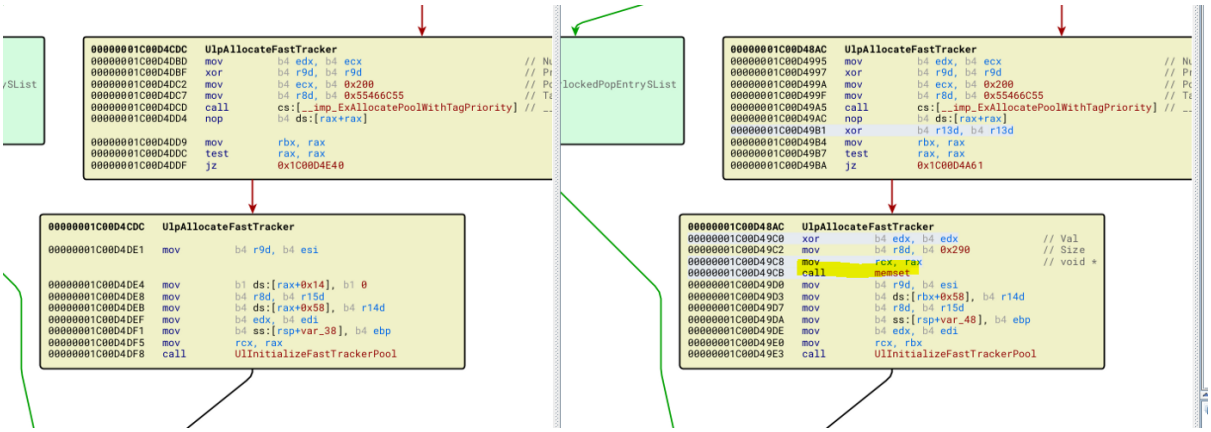

Figure 3: UlpAllocateFastTracker unpatched vs. patched version

UlPAllocateFastTracker is another interesting function that has undergone some adjustments. A number of base blocks have been changed in the patched version. Many calls to memset to reset memory stand out as notable changes. This is one method of solving memory corruption issues. Also, we see that more than one memset() is added with patched in UlPAllocateFastTracker, in this case we can say that it is done to minimize memory

corruption errors. If the system is under memory pressure, attacker-controlled data can be sprayed into the memory and appear in the newly created Tracker buffer.

There is a possibility of remote code execution because we have control of mapping any attacker-controlled memory. However, constructing such a remote code execution would necessitate more investigation into the Tracker fields' functions. The attacker would either need to saturate the RAM with phony MDLs and Tracker pointers (which may need another vulnerability that exposes kernel address information) or take advantage of the fact that additional fields in Tracker are not correctly set.

Scope of Impact

Table 1: Affected windows versions

Version Affected	Attention
Windows Server 2019 (Server Core Installation)	Windows 10 version 1909 (unaffected)
Windows Server 2019	Windows Server 2019 (Default configuration is not affected)
Windows 10 Version 21H2 for Arm64-based Systems	Windows 10 version 1809 (Default configuration is not affected)
Windows 10 Version 21H2 for 32-bit Systems	
Windows 11 for ARM64-based Systems	
Windows 11 for x64-based Systems	
Windows Server, version 20H2 (Server Core Installation)	
Windows 10 Version 20H2 for ARM64-based Systems	
Windows 10 Version 20H2 for 32-bit Systems	
Windows 10 Version 20H2 for x64-based Systems	
Windows Server 2022 (Server Core installation)	
Windows Server 2022	
Windows 10 Version 21H1 for 32-bit Systems	
Windows 10 Version 21H1 for ARM64-based Systems	

Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 21H2 for x64-based Systems	
Windows 10 Version 1809 for ARM64-based Systems	
Windows 10 Version 1809 for x64-based Systems	
Windows 10 Version 1809 for 32-bit Systems	

Mitigation

Microsoft has officially released an update to fix this vulnerability.

Fix Patch : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907

If you have an operating system with Windows Server 2019 or Windows 10 version 1809 and you have not downloaded the update yet, you can temporarily delete the "EnableTrailerSupport" in the DWORD registry.

Path : HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters

Conclusion

We need to update our operating systems with the official patch package recommended by Microsoft as soon as possible in order not to be harmed by this cyber security vulnerability that threatens Microsoft operating systems, especially Windows Servers. Considering the capabilities of this vulnerability, such as remote code execution and Denial-of-service (DoS) attacks, we must secure our systems as soon as possible.

Resources:

1- Lau, T. (2022, February 15). *Analysis of Microsoft CVE-2022-21907: Fortiguard Labs* . Fortinet Blog. Retrieved June 12, 2022, from https://www.fortinet.com/blog/threat-research/analysis-of-microsoft-cve-2022-21907

2- *Microsoft CVE-2022-21907: HTTP protocol stack remote code execution vulnerability*. Rapid7. (n.d.). Retrieved June 12, 2022, from https://www.rapid7.com/db/vulnerabilities/msft-cve-2022-21907/

3- *You are viewing this page in an unauthorized frame window.* NVD. (n.d.). Retrieved June 12, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2022-21907

4- *HTTP stack remote code execution vulnerability (CVE-2022-21907) alert*. NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. (2022, January 27). Retrieved June 12, 2022, from https://nsfocusglobal.com/http-stack-remote-code-execution-vulnerability-cve-2022-21907-alert/