CVSS: 9.8 (Critical)

# HTTP PROTOCOL STACK REMOTE CODE EXECUTION VULNERABILITY

By Six Degrees Cyber Security Operations Centre

Date of issue: 17.1.2022
CVE-2022-21907

## Executive Summary

**On 11th January 2022 (as part of patch Tuesday) Microsoft released patches for 97 CVE-numbered vulnerabilities, including a wormable remote code execution in Windows Server (CVE-2022-21907). This means an attacker could utilise the HTTP Protocol Stack (http.sys) on a server inside your network to run malicious code without asking for permission first.**

**The vulnerability has been given a 9.8 CVSSv3 score; patching affected servers should be prioritised immediately (Windows 10 and 11 and Server 2019 and 2022).**

**The flaw has not yet been exploited, but it has been rated as 'Exploitation More Likely' according to Microsoft's Exploitability Index. We would also like to remind you that similar vulnerabilities exist in Windows 7 and 8, as well as Server 2003 and 2008. However, as these are end of life they are no longer reported by Microsoft and no further patches are developed. If you currently operate with any of these legacy operating systems, we encourage you to discuss upgrade options with your account team as soon as possible.**

**Microsoft have retracted their Windows Server updates due to critical bugs. We will apply the update as soon as a patch has been released.**
**We will continue to apply patching for Windows 10 Desktops.**
**See below for more technical information.**

## Six Degrees Technical Review

Research teams have published information about a remote code execution vulnerability issue that has occurred in the HTTP protocol stack. Given that it's wormable, an exploit could self-propagate through a network with no user interaction. This can be exploited by sending specially crafted packets to a system using the HTTP protocol stack (http.sys) to process packets.

This affects systems that aren't servers or even running ISS (Internet Information Services) This is not an IIS vulnerability but a vulnerability in http.sys. http.sys is best described as the core HTTP engine inside IIS. But other software using http.sys and possibly exposing the vulnerability includes WinRM (Windows Remote Management) and WSDAPI (Web Services for Devices). For a quick list of processes using http.sys, open command line/PowerShell: **Netsh http show servicestate**. We recommend this to be done on each server.

**Non-Disclosure Statement**
This document contains intellectual property rights and copyright, which are proprietary to Six Degrees. The work and the information it contains are submitted for the purpose of making a proposal, fulfilling a contract or as marketing collateral. It is to be treated as confidential and shall not be used for any other purpose. It shall not be copied or disclosed to third parties, in whole or in part, without the prior written consent of Six Degrees.

The vulnerable Windows component in this issue is a Kernel Mode device driver used to process HTTP requests at high speed. http.sys isn't present in just server versions of Windows; it's also present in older OS versions Windows 7, Windows 8, and Windows 8.1. This means any desktop systems not being patched diligently are also vulnerable to this issue.

This vulnerability is the latest example of how software capabilities can be warped and weaponised. The CVE targets the HTTP trailer support feature, which allows a sender to include additional fields in a message to supply metadata, by providing a specially crafted message that can lead to remote code execution. **This makes CVE-2022-21907 a patching priority.**

**Vulnerable/affected systems:**

- Windows 10
- Windows 11
- Server 2019
- Server 2022

## Next Steps

If you benefit from our Managed OS service, we will apply this patch as part of your next scheduled patching run (if scheduled within the next week) or we will contact you shortly to get this booked in.

If you do not subscribe to our Managed OS service or are unable to patch as soon as possible, we recommend you take the below mitigation steps:

- Disable certain inactive features via the registry to improve security if the latest patch cannot be installed, or to mitigate this vulnerability prior to the patch being applied.
- Delete the DWORD registry value "EnableTrailerSupport" if present under:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters

**Note**: this mitigation only applies to Windows Server 2019 and Windows 10 version 1809, and does not apply to other affected versions of Windows; patching to the latest version is the only option. In Windows Server 2019 and Windows 10 version 1809, the HTTP Trailer Support feature that contains the vulnerability is not active by default.

Patching will also mitigate a myriad of other vulnerabilities that were disclosed. These can be seen in Annex A.

## References

https://krebsonsecurity.com/2022/01/wormable-flaw-leads-january-2022-patch-tuesday/
https://threatpost.com/microsoft-wormable-critical-rce-bug-zero-day/177564/
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21907
https://securityonline.info/cve-2022-21907-http-protocol-stack-remote-code-execution-vulnerability/
https://www.infoworld.com/article/2910262/4-no-bull-facts-about-microsofts-http-sys-vulnerability.html
https://isc.sans.edu/forums/diary/A+Quick+CVE202221907+FAQ+work+in+progress/28234/

**Non-Disclosure Statement**
This document contains intellectual property rights and copyright, which are proprietary to Six Degrees. The work and the information it contains are submitted for the purpose of making a proposal, fulfilling a contract or as marketing collateral. It is to be treated as confidential and shall not be used for any other purpose. It shall not be copied or disclosed to third parties, in whole or in part, without the prior written consent of Six Degrees.

## Annex A

The table below provides a very high-level overview of the vulnerabilities addressed in the patch Tuesday release from Microsoft. However, for further information and links to the security updates please review https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21907.

| CVE | Description |
|---|---|
| CVE-2022-21840<br>CVSS 8.8 | Microsoft Office-related RCE bug that does not does not display warning dialog boxes when opening specially crafted file.<br>No patch yet for Office 2019 for Mac and Microsoft Office LTSC for Mac 2021 (CVSS 8.8). |
| CVE-2022-21846<br>CVSS 9.0 | Critical RCE bug in Microsoft Exchange Server requiring the attacker to be network adjacent (already on the network). |
| CVE-2021-22947<br>Not yet determined | An open-source cURL library used by Windows to transfer data using various network protocols. It allows RCE leading to man-in-the-middle (MiTM) attacks. |
| CVE-2022-21857<br>CVSS 8.8 | Allows elevation of privileges across an Active Directory trust boundary under certain conditions. This could be used for lateral movement, although it requires a certain level of privileges initially which would indicate an insider threat or an attacker with a prior foothold in the network. |
| CVE-2022-21833<br>CVSS 7.8 | A privilege-escalation issue in the Virtual Machine IDE Drive. To exploit it, a threat actor would need to gain access to an underprivileged account, such as through an unsecure user password or an account with minimal access controls, to expose this vulnerability. |
| CVE-2022-21912<br>CVE-2022-21898<br>Both CVSS 7.8 | Two critical issues in the DirectX Graphics Kernel; viewing a specially crafted media file could result in code execution. This can allow attackers to take full control of a system within the network and spread to other systems. Components using the DirectX Kernel are likely present in most systems. |
| CVE-2022-21917<br>CVSS 7.8 | HEVC Video Extensions. Successful exploitation would require an attacker to bait an authenticated user into opening a maliciously crafted media file, which would result in remote code execution on the victim's machine. Microsoft does not provide mitigation recommendations aside from patching. |
| CVE-2021-36976<br>Not yet determined | Libarchive remote code execution vulnerability, the technical details are not yet publicly available, exploitation requires authentication. |
| CVE-2022-21874<br>CVSS 7.8 | Windows Security Center API Remote Code Execution Vulnerability. The exploitation doesn't require any form of authentication. Successful exploitation requires user interaction by the victim. |
| CVE-2022-21919<br>CVSS 7.0 | Windows User Profile Service Elevation of Privilege Vulnerability. The attack may be initiated remotely. The requirement for exploitation is a simple authentication. |
| CVE-2022-21839<br>CVSS 6.1 | Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability. This vulnerability can be exploited remotely following authentication and will result in endpoint denial of service. |
| CVE-2022-21836<br>CVSS 7.8 | Windows Certificate Spoofing Vulnerability. This can be exploited remotely and requires authentication. An exploit is not publicly available. |
| CVE-2022-21849<br>CVSS 9.8 | Windows IKE Extension Remote Code Execution Vulnerability. Microsoft has published limited information about this new vulnerability, but Six Degrees is aware and will stay vigilant when new threat intel has been released and keep you updated. |

**Non-Disclosure Statement**

This document contains intellectual property rights and copyright, which are proprietary to Six Degrees. The work and the information it contains are submitted for the purpose of making a proposal, fulfilling a contract or as marketing collateral. It is to be treated as confidential and shall not be used for any other purpose. It shall not be copied or disclosed to third parties, in whole or in part, without the prior written consent of Six Degrees.