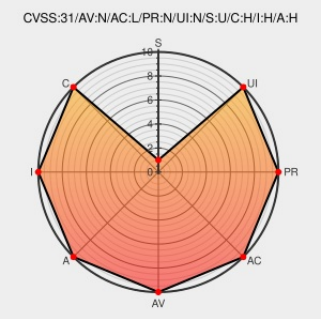
# CVE-2021-31166

Published on: 05/11/2021 12:00:00 AM UTC

Last Modified on: 08/02/2023 12:15:00 AM UTC

## CVE-2021-31166

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Windows 10 from Microsoft contain the following vulnerability:

HTTP Protocol Stack Remote Code Execution Vulnerability

CVE-2021-31166 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Microsoft** - **Windows 10 Version 2004** version **< 10.0.19041.982**

Affected Vendor/Software: **Microsoft** - **Windows Server version 2004** version **< 10.0.19041.982**

Affected Vendor/Software: **Microsoft** - **Windows 10 Version 20H2** version **< 10.0.19042.982**

Affected Vendor/Software: **Microsoft** - **Windows Server version 20H2** version **< 10.0.19042.982**

### CVSS3 Score: 9.8 - CRITICAL

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Microsoft HTTP Protocol Stack Remote Code Execution ≈ Packet Storm | packetstormsecurity.com text/html | MISC packetstormsecurity.com/files/162722/Microsoft-HTTP-Protocol-Stack-Remote-Code-Execution.html |
| Security Update Guide - Microsoft Security Response Center | portal.msrc.microsoft.com text/html | MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166 |



## Related QID Numbers

91762 Microsoft Windows Security Update for May 2021

91767 Microsoft Windows HTTP Protocol Stack Remote Code Execution Vulnerability - May 2021

## Exploit/POC from Github

Proof of concept for CVE-2021-31166, a remote HTTP.sys use-after-free triggered remotely.

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Microsoft | Windows 10 | 2004 | All | All | All |
| Operating System | Microsoft | Windows 10 | 20h2 | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | 2004 | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | 20h2 | All | All | All |

cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:2004:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:20h2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @kpyke | In case you're wondering what to prioritize in today's Microsoft Tuesday patch set, the answer is CVE-2021-31166.… twitter.com/i/web/status/1… | 2021-05-11 17:27:16 |

| | | |
|---|---|---|
| @0x009AD6_810 | 今月の最優先はこれかな msrc.microsoft.com/update-guide/j… CVE-2021-31166 HTTPプロトコルスタック Ring0 RCE (認証無しなのでワーム化も可能) | 2021-05-11 17:36:38 |
| @nluedtke1 | CVE-2021-31166 - Wormable RCE in HTTP Protocol stack. | 2021-05-11 17:52:28 |
| @d1wn | Ямо. HTTP Protocol Stack Remote Code Execution Vulnerability CVE-2021-31166 | 2021-05-11 18:00:12 |
| @yuuturn5 | おー。 msrc.microsoft.com/update-guide/v… HTTP プロトコル スタックのリモートでコードが実行される脆弱性 CVE-2021-31166 | 2021-05-11 18:21:44 |
| @tamosan | 今月のWUで気になったもの。http[.]sysの問題ということで2015年のMS15-034を思い出しますね。なお20H1以降のWin10系対象：CVE-2021-31166 - セキュリティ更新プログラム ガイド - Micr… twitter.com/i/web/status/1… | 2021-05-11 19:08:43 |
| @spovolny | We'll have a quick summary blog on the vulnerability CVE-2021-31166 coming soon, but the tl;dr is - Patch quickly :) twitter.com/Bulldog_Palm/s… | 2021-05-11 19:15:29 |
| @CVEreport | CVE-2021-31166 : HTTP Protocol Stack Remote Code Execution Vulnerability... cve.report/CVE-2021-31166 | 2021-05-11 19:20:43 |
| @GossiTheDog | Kevin's Lame Review of May 2021's Patch Tuesday, thread. CVE-2021-31166 - RCE in HTTP Protocol (think mini IIS).... twitter.com/i/web/status/1… | 2021-05-11 20:12:43 |
| @McAfee_Labs | The following statement is from @spovolny, Head of Advanced Threat Research and Principle Engineer. CVE-2021-31166… twitter.com/i/web/status/1… | 2021-05-11 20:19:34 |
| @edelahozuah | @GossiTheDog not even the HTTP RCE vuln CVE-2021-31166? | 2021-05-11 20:45:18 |
| @ipssignatures | Talos has a protection/signature/rule for the vulnerability CVE-2021-31166. feedproxy.google.com/~r/Snort/~3/AT… The vuln may no… twitter.com/i/web/status/1… | 2021-05-11 21:04:02 |
| @ipssignatures | The vuln CVE-2021-31166 has a tweet created 0 days ago and retweeted 12 times. twitter.com/kpyke/status/1… #Sla7log4erxrzm | 2021-05-11 21:04:03 |
| @ka0com | Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166) tenable.com/blog/microsoft… | 2021-05-11 21:49:59 |
| @ipssignatures | The vuln CVE-2021-31166 has a tweet created 0 days ago and retweeted 12 times. twitter.com/GossiTheDog/st… #pow1rtrtwwcve | 2021-05-11 23:06:00 |
| @exploding_box | CVE-2021-31166優先だろうに... | 2021-05-12 01:04:19 |
| @ohhara_shiojiri | "CVE-2021-31166 – Wormable" | 2021-05-12 01:17:45 |
| @tongson | windows::http.sys::RCE::CVE-2021-31166 | 2021-05-12 02:03:49 |
| @EurekaBerry | 今月メモ① CVE-2021-31166 HTTP.sysの 認証なしユーザー操作なしのRCE CVSS 9.8。MS内部調査で見つかった脆弱性で悪用公開は現在無し。が、ワーム化が可能な脆弱性のため悪用に好まれるタイプであり、早め… twitter.com/i/web/status/1… | 2021-05-12 02:19:37 |
| @blackorbird | HTTP Protocol Stack Remote Code Execution Vulnerability(CVE-2021-31166) #wormable Exploitation More Likely… twitter.com/i/web/status/1… | 2021-05-12 02:48:05 |
| @bluehexagonai | Read the latest Blue Hexagon Threat Advisory about CVE-2021-31166 that can lead to #Remotecodeexecution and is pote… twitter.com/i/web/status/1… | 2021-05-12 04:14:11 |
| @thomasfricke | Wormable msrc.microsoft.com/update-guide/e… | 2021-05-12 05:43:24 |
| @pkraszewski | CVE-2021-31166 "HTTP Protocol Stack Remote Code Execution Vulnerability" "This vulnerability allows an unauthentica… twitter.com/i/web/status/1… | 2021-05-12 08:02:32 |

| | | |
|---|---|---|
| @secuninja | CVE-2021-31166 #new #patchnow | 2021-05-12 08:24:32 |
| @mpontoiz | Everyone should be focused on patching CVE-2021-31166 ASAP. lnkd.in/euPSWbC | 2021-05-12 08:54:46 |
| @the_yellow_fall | CVE-2021-31166: HTTP Protocol Stack Remote Code Execution Vulnerability meterpreter.org/cve-2021-31166… #info #news #tech | 2021-05-12 09:46:17 |
| @Art_Capella | Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166) ow.ly/7oah102JsRd | 2021-05-12 11:39:49 |
| @t31m0 | Tendencias de hoy ... msrc.microsoft.com/update-guide/v… https://t.co/3sJBQmDy15 | 2021-05-12 12:36:29 |
| @grobi_grobsen | remote code execution, hübsch. msrc.microsoft.com/update-guide/e… | 2021-05-12 12:57:35 |
| @immersivelabs | "For ransomware operators, CVE-2021-31166 is a prime target for exploitation and wormable exploits should always be… twitter.com/i/web/status/1… | 2021-05-12 13:06:09 |
| @autumn_good_35 | 今月は、やはりパケット送りつけるだけでのRCE（CVE-2021-31166）ですが、ユーザ操作不要なVisual StudioのRCE（CVE-2021-27068）も詳細が気になります。 スクリプトエンジンのRCE（CVE-2… twitter.com/i/web/status/1… | 2021-05-12 13:20:12 |
| @tempest_sec | Entre estas, destaque para a vulnerabilidade CVE-2021-31166 (CVSS 9.8), uma falha de execução remota de comandos na… twitter.com/i/web/status/1… | 2021-05-12 13:40:22 |
| @BullStallcup | Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166) ow.ly/E0IH102JtuN | 2021-05-12 13:43:35 |
| @Dinosn | HTTP Protocol Stack Remote Code Execution Vulnerability msrc.microsoft.com/update-guide/v… | 2021-05-12 14:40:13 |
| @YejarlaMadhava | HTTP Protocol Stack Remote Code Execution Vulnerability msrc.microsoft.com/update-guide/v… | 2021-05-12 14:44:01 |
| @vincefalconi | i was busy reading about Frag Attack yesterday (all of which was whoosh over my head) and completely missed CVE-2021-31166. OH BOY. | 2021-05-12 17:00:26 |
| @brycea | Important #PatchTuesday -- "By all accounts, the most pressing priority this month is CVE-2021-31166, a Windows 10… twitter.com/i/web/status/1… | 2021-05-12 18:03:17 |
| @qm_ssj4 | So anyone only looking at IIS server for http.sys CVE-2021-31166 your not doing it right. https://t.co/6UKVOFqrTj | 2021-05-12 18:10:13 |
| @Har_sia | CVE-2021-31166 har-sia.info/CVE-2021-31166… #HarsiaInfo | 2021-05-12 18:23:02 |
| @morodog | #News CVE-2021-31166: HTTP Protocol Stack Remote Code Execution Vulnerability: On May 11, Microsoft officially rele… twitter.com/i/web/status/1… | 2021-05-12 18:41:09 |
| @CharlesDardaman | Neat a new "wormable" vuln in http.sys msrc.microsoft.com/update-guide/e… | 2021-05-12 20:58:31 |
| @jpierre76 | Patch Tesday, plusieurs failles ont été colmaté ainsi que le ver (CVE-2021-31166) dans la couche HTTP.… twitter.com/i/web/status/1… | 2021-05-12 21:39:36 |
| @morodog | CVE-2021-31166: HTTP Protocol Stack Remote Code Execution Vulnerability: On May 11, Microsoft officially released t… twitter.com/i/web/status/1… | 2021-05-12 22:56:06 |
| @enz_3ura | マイクロソフト月例Updateで気になったもの。 HTTPプロトコルスタックリモートコード実行の脆弱性 (CVE-2021-31166) 細工したパケットを送信することで悪用可能とあるが、対象がWin10のWebサーバ。外部公開は… twitter.com/i/web/status/1… | 2021-05-13 00:55:28 |
| @enz_3ura | HTTPプロトコルスタックリモートコード実行の脆弱性 (CVE-2021-31166) msrc.microsoft.com/en-US/security… | 2021-05-13 00:56:26 |
| @ShankerSareen | Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166) | 2021-05-13 |

| | | |
|---|---|---|
| | ow.ly/yAik102JwJ5 | 03:21:01 |
| @Raj_Samani | Details on CVE-2021-31166 - "As HTTP.SYS is implemented as a kernel driver, exploitation of this bug will result i… twitter.com/i/web/status/1… | 2021-05-13 05:45:00 |
| @cyber_advising | CVE-2021-31166: HTTP Protocol Stack Remote Code Execution Vulnerability msrc.microsoft.com/update-guide/v… | 2021-05-13 06:08:07 |
| @shellist_ | "wormable RCE (CVE-2021-31166) in the HTTP protocol stack." twitter.com/thehackersnews… https://t.co/JE4Rd87PmI | 2021-05-13 07:13:03 |
| @gaetanoz | CVE-2021-31166 - Security Update Guide - Microsoft - HTTP Protocol Stack Remote Code Execution Vulnerability msrc.microsoft.com/update-guide/v… | 2021-05-13 07:35:18 |
| @Anastasis_King | CVE-2021-31166 : HTTP Protocol Stack Remote Code Execution Vulnerability Wormable RCE in HTTP Protocol stack(http.… twitter.com/i/web/status/1… | 2021-05-13 08:33:54 |
| @AlicePintori | Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166) ow.ly/BBrR102Jxjk | 2021-05-13 09:03:14 |
| @ipssignatures | It's new to me that CheckPoint has a protection/signature/rule for the vulnerability CVE-2021-31166.… twitter.com/i/web/status/1… | 2021-05-13 11:02:01 |
| @ipssignatures | I know one more IPS that has a protection/signature/rule for the vulnerability CVE-2021-31166. ipssignatures.appspot.com/?cve=CVE-2021-… #Sla7log4erxrzm | 2021-05-13 11:02:01 |
| @dansantanna | Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166) ow.ly/UKLe102JyLz | 2021-05-13 11:32:01 |
| @HostileSpectrum | Lost in the week, CVE-2021-31166 wormable http.sys RCE perfectly encapsulates offensive advantage in one bug. Where… twitter.com/i/web/status/1… | 2021-05-13 12:40:57 |
| @ipssignatures | It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2021-31166. … twitter.com/i/web/status/1… | 2021-05-13 17:02:02 |
| @ipssignatures | I know 2 other IPSs that have protections/signatures/rules for the vulnerability CVE-2021-31166. ipssignatures.appspot.com/?cve=CVE-2021-… #Sla7log4erxrzm | 2021-05-13 17:02:02 |
| @Har_sia | CVE-2021-31166 har-sia.info/CVE-2021-31166… #HarsiaInfo | 2021-05-13 18:23:02 |
| @windsheep_ | Ok, HTTP Protocol Stack Remote Code Execution Vulnerability on Windows. 2021. In the kernel. msrc.microsoft.com/update-guide/e… | 2021-05-13 21:00:28 |
| /r/sysadmin | CVE-2021-31166 – Windows HTTP Protocol Stack Remote Code Execution Vulnerability | 2021-05-11 23:52:05 |
| /r/blueteamsec | CVE-2021-31166: Microsoft Windows HTTP Protocol Stack Remote Code Execution Vulnerability - blue screens a target currently (i.e. does not achieve full RCE) | 2021-05-17 07:57:40 |
| /r/CyberNews | PoC exploit code for Windows CVE-2021-31166 bug | 2021-05-17 14:39:19 |
| /r/InfoSecNews | Expert released PoC exploit code for Windows CVE-2021-31166 bug | 2021-05-17 17:49:49 |
| /r/virtualradarserver | Windows VRS Users and May 2021 Windows Updates | 2021-05-17 20:29:36 |
| /r/cybersecurity | 0vercl0k/CVE-2021-31166 | 2021-05-18 03:08:58 |
| /r/ReverseEngineering | CVE-2021-31166: A Wormable Code Execution Bug in HTTP.sys | 2021-05-18 15:59:04 |
| /r/sysadmin | Windows Exploit in http-sys: Proof-of-Concept publicly available now | 2021-05-19 12:19:31 |
| /r/windows | New vulnerability CVE-2021-31166 20h2 and 2004 versions. | 2021-05-22 |

| | | |
|---|---|---|
| | | 00:48:11 |
| /r/InfoSecNews | CVE-2021-31166 Windows HTTP flaw also impacts WinRM servers | 2021-05-24 10:49:11 |

← Previous ID

Next ID→