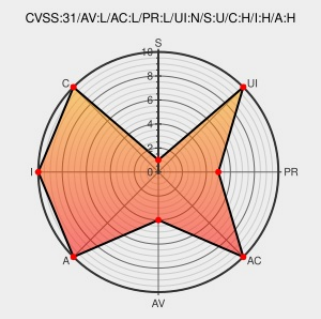
# CVE-2021-26900

Published on: 03/11/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 04:04:00 PM UTC

## CVE-2021-26900

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




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

Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26863, CVE-2021-26875, CVE-2021-27077.

CVE-2021-26900 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 7.8 - HIGH

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

### CVSS2 Score: 7.2 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Security Update Guide - Microsoft Security Response Center | Patch, Vendor Advisory, portal.msrc.microsoft.com, text/html | MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26900 |

ZDI-21-331 | Zero Day Initiative

Third Party Advisory
www.zerodayinitiative.com
text/html

MISC www.zerodayinitiative.com/advisories/ZDI-21-331/



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Microsoft | Windows 10 | 1909 | All | All | All |
| Operating System | Microsoft | Windows 10 | 2004 | All | All | All |
| Operating System | Microsoft | Windows 10 | 20h2 | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | 1909 | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | 20h2 | All | All | All |

cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:microsoft:windows_server_2016:1909:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @ipssignatures | The vuln CVE-2021-26900 has a tweet created 0 days ago and retweeted 10 times. twitter.com/Dinosn/status/… #pow1rtrtwwcve | 2021-05-05 17:06:00 |
| @Har_sia | CVE-2021-26900 har-sia.info/CVE-2021-26900… #HarsiaInfo | 2021-05-05 18:25:02 |
| @Hoorge | CVE-2021-26900: Privilege Escalation Via a Use After Free Vulnerability In win32k bit.ly/3okCOx3 | 2021-05-15 13:32:01 |
| @d0lph1n98 | CVE-2021-26411 + CVE-2021-26900 chain https://t.co/4niuMn2p89 | 2021-07-09 05:53:32 |
| @ipssignatures | The vuln CVE-2021-26900 has a tweet created 0 days ago and retweeted 14 times. twitter.com/d0lph1n98/stat… #pow1rtrtwwcve | 2021-07-09 11:06:01 |

| | | |
|---|---|---|
| @0day_sniper | Analysis of #DirectComposition Binding and Tracker object vulnerability. CVE-2020-1381 CVE-2021-26900 CVE-2021-2686… twitter.com/i/web/status/1… | 2021-08-14 14:36:48 |
| /r/lowlevel | CVE-2021-26900: Privilege Escalation Via a Use After Free Vulnerability In win32k | 2021-05-04 17:28:56 |
| /r/ReverseEngineering | CVE-2021-26900: Privilege Escalation Via a Use After Free Vulnerability In win32k - includes root cause analysis and PoC | 2021-05-04 17:07:25 |

← Previous ID

Next ID→