



CVE-2020-1381

Published on: 07/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:45 PM UTC

CVE-2020-1381

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows 10](#) from [Microsoft](#) contain the following vulnerability:

An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1382.

CVE-2020-1381 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: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1381

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All

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

cpe:2.3:o:microsoft:windows_server_2016:1903:*****:
cpe:2.3:o:microsoft:windows_server_2016:1909:*****:
cpe:2.3:o:microsoft:windows_server_2016:2004:*****:
cpe:2.3:o:microsoft:windows_server_2016:1903:*****:
cpe:2.3:o:microsoft:windows_server_2016:1909:*****:
cpe:2.3:o:microsoft:windows_server_2016:2004:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @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/fortinet	Threat Protection Statistics	2022-10-07 09:29:23

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)