



CVE-2020-1020

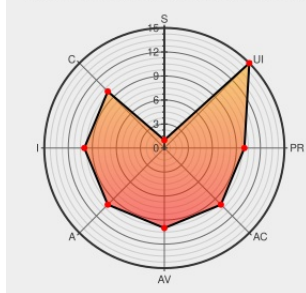
Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-1020

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely,

aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0938.

CVE-2020-1020 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	CVE	@MISC - cve.mitre.org/cve/2020/1020/MSRC-2020-1020-microsoft.com/en-US/security/advisories/CVE-2020-1020

[No Description Provided](#)[Patch](#)[Vendor Advisory](#)[portal.msrc.microsoft.com](#)[text/html](#)[MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Windows Font Driver Type 1 VToHOrigin stack corruption

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	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	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	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 7	-	sp1	All	All

System						
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	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	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	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 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
cpe:2.3:o:microsoft:windows_10:-:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1607:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1709:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1803:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1809:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1903:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1909:****:*:*:						
cpe:2.3:o:microsoft:windows_10:-:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1607:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1709:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1803:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1809:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1903:****:*:*:						
cpe:2.3:o:microsoft:windows_10:1909:****:*:*:						
cpe:2.3:o:microsoft:windows_7:-:sp1:****:*:*:						
cpe:2.3:o:microsoft:windows_7:-:sp1:****:*:*:						
cpe:2.3:o:microsoft:windows_8.1:-:****:*:*:						
cpe:2.3:o:microsoft:windows_8.1:-:****:*:*:						
cpe:2.3:o:microsoft:windows_rt_8.1:-:****:*:*:						
cpe:2.3:o:microsoft:windows_rt_8.1:-:****:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:****:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:****:itanium:*:						
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:****:x64:*:						
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:****:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:****:itanium:*:						

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2016:1803:*:*:*:*:*:
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:-:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2016:1803:*:*:*:*:*:
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_2019:-:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @yuyuyu_sec	CVE-2020-1020も初めて見たような ぱっと見大丈夫そうだけど、Twitter登録したのが今年の4月であるだけでだいぶ警戒してしまう...人間不信	2021-06-09 12:05:30
 /r/SCCM	How do I find CVE updates in SCCM	2021-05-27 19:12:10

[← 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](#)