

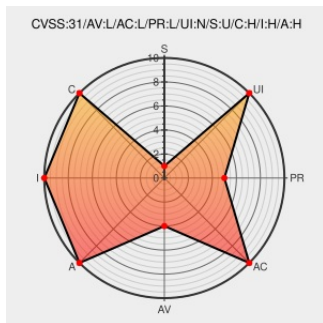


CVE-2020-1337

Published on: 08/17/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-1337

[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 Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'.

CVE-2020-1337 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
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	N/A N/A

Microsoft Windows Local Spooler Bypass ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/160028/Microsoft-Windows-Local-Spooler-Bypass.html
Microsoft Spooler Local Privilege Elevation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/160993/Microsoft-Spooler-Local-Privilege-Elevation.html

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

CVE-2020-1337 Windows Print Spooler Privilege Escalation

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	2004	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 10	2004	All	All	All
Operating System	Microsoft	Windows 7	sp1	All	All	All
Operating System	Microsoft	Windows 7	sp1	All	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	-	sp2	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	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	-	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 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_10:2004:*:*:*:*:*:						
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_10:2004:*:*:*:*:*:						
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:~::~~::~~::~~::~~::~~::~~::x64:~::
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:~::~~::~~::~~::~~::~~::~~::
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_2016:1903:~::~~::~~::~~::~~::~~::~~::
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:-:~::~~::~~::~~::~~::~~::~~::
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_2019:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:o:microsoft:windows_server_2019:-:~::~~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔒 @pwnwikiorg	CVE-2020-1337 Microsoft Spooler 本地權限提升漏洞 pwnwiki.org/index.php?titl...	2021-05-31 04:07:42
🔒 @JamesHare_BFX	@ExAndroidDev wait so CVE-2020-1337 is not actually patched it is still, in fact, 1337?	2021-06-24 20:36:34
🔒 @CyberWarship	sailay1996/cve-2020-1337-poc poc for CVE-2020-1337 (Windows Print Spooler Elevation of Privilege) #pentest... twitter.com/i/web/status/1...	2021-06-28 13:40:05
🔒 @infowaropcenter	Top story: GitHub - sailay1996/cve-2020-1337-poc: poc for CVE-2020-1337 (Windows Print Spooler Elevation of Privile... twitter.com/i/web/status/1...	2021-06-28 23:12:02
🔒 @infowaropcenter	Top story's from my Newspaper GitHub - sailay1996/cve-2020-1337-poc: poc for CVE-2020-1337 (Windows Print Spooler E... twitter.com/i/web/status/1...	2021-06-28 23:32:26
🔒 @ptracesecurity	poc for CVE-2020-1337 (Windows Print Spooler Elevation of Privilege	2021-06-30

	github.com/sailay1996/cve... #Pentesting #CVE... twitter.com/i/web/status/1...	23:32:07
🔒 @jc0f0116	@ptracesecurity cve-2020-1048 -> cve-2020-1337 -> cve-17001... and still even now are not careful about patching variants...	2021-06-30 23:57:55
🔒 @ipssignatures	The vuln CVE-2020-1337 has a tweet created 0 days ago and retweeted 13 times. twitter.com/ptracesecurity... #pow1rtrtwwcve	2021-07-01 03:06:00
🔒 @CyberWarship	math1as/CVE-2020-1337-exploit in the patch of CVE-2020-1048, Microsoft add the validation code of portname on XcvD... twitter.com/i/web/status/1...	2021-07-12 13:40:02
🔒 @onuroktay	Microsoft #PrintNightmare için Poc github.com/sailay1996/cve... #vulnerabilities	2021-07-13 06:26:50
🔒 @ipssignatures	The vuln CVE-2020-1337 has a tweet created 21 days ago and retweeted 10 times. twitter.com/CyberWarship/s... #pow1rtrtwwcve	2021-08-02 17:06:01
🔒 @Wh0_D1s_1	Windows Privilege Escalation: SpoolFool Патчили, фиксели CVE-2020-1048 и CVE-2020-1337, а дыра осталась. Отличный... twitter.com/i/web/status/1...	2022-03-25 15:16:49
← Previous ID Next ID →		

© CVE.report 2023 🔒 N |

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](#)