



CVE-2019-1040

Published on: 06/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:47 PM UTC

CVE-2019-1040

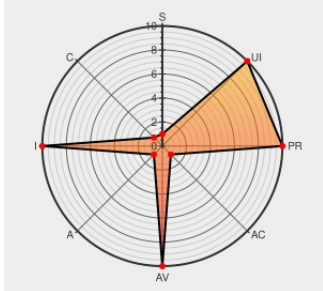
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N



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

A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.

CVE-2019-1040 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1040

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

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	1703	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	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	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 7	-	sp1	All	All
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

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:-:*****:
cpe:2.3:o:microsoft:windows_10:1607:*****:
cpe:2.3:o:microsoft:windows_10:1703:*****:
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_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:-:*****:
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_2019:-:*****:
cpe:2.3:o:microsoft:windows_server_2019:-:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @aubrey_lab	dirkjanm.io/exploiting-CVE...	2021-06-05 17:15:21
 @_nwodtuhs	@thecyberlama yup, make sure your domain controllers are patched against CVE-2019-1040 and CVE-2019-1166, make sure... twitter.com/i/web/status/1...	2021-07-21 13:36:15
 @GossiTheDog	@_nwodtuhs Do patches for CVE-2019-1040 and CVE-2019-1166 actually fix this?	2021-07-21 22:07:41
 @_nwodtuhs	But if you have DC2 not patched against CVE-2019-1040, LDAPS supported with Channel Binding not enabled, and are in... twitter.com/i/web/status/1...	2021-07-22 07:21:19
 @gladiatx0r	@_nwodtuhs Does pywhisker (or your impacket pr) attempt the signing bypass (cve-2019-1040) automatically? Seems to from the ss above.	2021-08-13 12:49:49
 /r/sysadmin	25 vulnerabilities exploited by Chinese state-sponsored hackers	2020-10-21 11:41:34
 /r/cybersecurity	25 vulnerabilities exploited by Chinese state-sponsored hackers	2020-10-21 11:37:21
 /r/cybersecurity	NTLM Relay Attack PetitPotam: What We Know So Far	2021-07-27 01:11:01

[← 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](#)