



CVE-2020-16938

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:50 PM UTC

CVE-2020-16938

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

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



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

An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16901.

CVE-2020-16938 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Microsoft - Windows 10 Version 2004 for 32-bit Systems** version

Affected Vendor/Software: **Microsoft - Windows 10 Version 2004 for ARM64-based Systems** version

Affected Vendor/Software: **Microsoft - Windows 10 Version 2004 for x64-based Systems** version

Affected Vendor/Software: **Microsoft - Windows Server, version 2004 (Server Core installation)** version

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

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-2020-16938

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

Bypassing NTFS permissions to read any files as unprivileged user.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	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_10:2004:*****:.*:						
cpe:2.3:o:microsoft:windows_server_2016:2004:*****:.*:						
cpe:2.3:o:microsoft:windows_server_2016:2004:*****:.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @jonasLyk	@mcohmi CVE-2020-16938	2021-12-21 21:05:28

[← 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](#)