



# NATIONAL VULNERABILITY DATABASE



## VULNERABILITIES

## CVE-2021-1675 Detail

### Description

Windows Print Spooler Remote Code Execution Vulnerability

### Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

#### CVSS 3.x Severity and Vector Strings:



**CNA:** Microsoft Corporation

**Base Score:** 7.8 HIGH

**Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

# References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites 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 web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to [nvd@nist.gov](mailto:nvd@nist.gov).


Hyperlink	Resource
<a href="http://packetstormsecurity.com/files/163349/Microsoft-PrintNightmare-Proof-Of-Concept.html">http://packetstormsecurity.com/files/163349/Microsoft-PrintNightmare-Proof-Of-Concept.html</a>	Third Party Advisory VDB Entry
<a href="http://packetstormsecurity.com/files/163351/PrintNightmare-Windows-Spooler-Service-Remote-Code-Execution.html">http://packetstormsecurity.com/files/163351/PrintNightmare-Windows-Spooler-Service-Remote-Code-Execution.html</a>	Third Party Advisory VDB Entry
<a href="http://packetstormsecurity.com/files/167261/Print-Spooler-Remote-DLL-Injection.html">http://packetstormsecurity.com/files/167261/Print-Spooler-Remote-DLL-Injection.html</a>	Exploit Third Party Advisory VDB Entry
<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675</a>	Patch Vendor Advisory
<a href="https://www.kb.cert.org/vuls/id/383432">https://www.kb.cert.org/vuls/id/383432</a>	Third Party Advisory US Government Resource

## This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and [Known Exploited Vulnerabilities Catalog](#) for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Microsoft Windows Print Spooler Remote Code Execution Vulnerability	11/03/2021	11/17/2021	Apply updates per vendor instructions.

## Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-Other	Other	 NIST

# Known Affected Software Configurations [Switch to CPE](#)

## 2.2

### Configuration 1 ([hide](#))

 <b>cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.10240.18967
 <b>cpe:2.3:o:microsoft:windows_10_1607:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.14393.4467
 <b>cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.17763.1999
 <b>cpe:2.3:o:microsoft:windows_10_1909:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.18363.1621
 <b>cpe:2.3:o:microsoft:windows_10_2004:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.19041.1052
 <b>cpe:2.3:o:microsoft:windows_10_20h2:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.19042.1052
 <b>cpe:2.3:o:microsoft:windows_10_21h1:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	Up to (excluding) 10.0.19043.1052
 <b>cpe:2.3:o:microsoft:windows_7::-sp1:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	
 <b>cpe:2.3:o:microsoft:windows_8.1::-:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	
 <b>cpe:2.3:o:microsoft:windows_rt_8.1::-:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	

 <b>cpe:2.3:o:microsoft:windows_server_2004:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	<b>Up to (excluding) 10.0.19041.1052</b>
 <b>cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	
 <b>cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*x64:*</b> <a href="#">Show Matching CPE(s)</a> ▼	
 <b>cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	
 <b>cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	
 <b>cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	<b>Up to (excluding)</b>



**HEADQUARTERS**

100 Bureau Drive  
Gaithersburg, MD 20899  
(301) 975-2000

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

**Incident Response Assistance and Non-NVD  
Related**

**Technical Cyber Security Questions:**

US-CERT Security Operations Center  
Email: [soc@us-cert.gov](mailto:soc@us-cert.gov)  
Phone: 1-888-282-0870

[Site Privacy](#) | [Accessibility](#) | [Privacy Program](#) | [Copyrights](#) | [Vulnerability Disclosure](#) | [No Fear Act Policy](#) | [FOIA](#) | [Environmental Policy](#) | [Scientific Integrity](#) | [Information Quality Standards](#) | [Commerce.gov](#) | [Science.gov](#) | [USA.gov](#)