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

QUICK INFO

CVE Dictionary Entry:
CVE-2021-1675

NVD Published Date:
06/08/2021

NVD Last Modified:
07/29/2024

Source:
Microsoft Corporation

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.

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

cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.10240.18967**
cpe:2.3:o:microsoft:windows_10_1607:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.14393.4467**
cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.17763.1999**
cpe:2.3:o:microsoft:windows_10_1909:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.18363.1621**
cpe:2.3:o:microsoft:windows_10_2004:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.19041.1052**
cpe:2.3:o:microsoft:windows_10_20h2:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.19042.1052**
cpe:2.3:o:microsoft:windows_10_21h1:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.19043.1052**
cpe:2.3:o:microsoft:windows_7:-:sp1:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_server_2004:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.19041.1052**
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.14393.4467**
cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding) 10.0.17763.1999**

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

11 change records found show changes

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

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
Phone: 1-888-282-0870