NIST

NVD MENU

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2021-34527 Detail

Description

<p>A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.</p> <p>UPDATE July 7, 2021: The security update for Windows Server 2012, Windows Server 2016 and Windows 10, Version 1607 have been released. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. If you are unable to install these updates, see the FAQ and Workaround sections in this CVE for information on how to help protect your system from this vulnerability.</p> <p>In addition to installing the updates, in order to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined (<strong>Note</strong>: These registry keys do not exist by default, and therefore are already at the secure setting.), also that your Group Policy setting are correct (see FAQ):</p> <ul> <li>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint</li>

<li>NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)</li> <li>UpdatePromptSettings = 0 (DWORD) or not defined (default setting)</li> </ul> <p><strong>Having NoWarningNoElevationOnInstall set to 1 makes your system vulnerable by design.</strong></p> <p>UPDATE July 6, 2021: Microsoft has completed the investigation and has released security updates to address this vulnerability. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. If you are unable to install these updates, see the FAQ and Workaround sections in this CVE for information on how to help protect your system from this vulnerability. See also <a href="https://support.microsoft.com/topic/31b91c02-05bc-4ada-a7ea-183b129578a7">KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates</a>.</p> <p>Note that the security updates released on and after July 6, 2021 contain protections for CVE-2021-1675 and the additional remote code execution exploit in the Windows Print Spooler service known as “PrintNightmare”, documented in CVE-2021-34527.</p>

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:** **8.8 HIGH**

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/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.

Hyperlink	Resource

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-2021-34527	Mitigation Patch Vendor Advisory

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	07/20/2021	Apply updates per vendor instructions.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-269	Improper Privilege Management	NVD 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) 10.0.10240.18969**
cpe:2.3:o:microsoft:windows_10_1607:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.14393.4470**
cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.17763.2029**
cpe:2.3:o:microsoft:windows_10_20h2:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding)**

	10.0.19042.1083
cpe:2.3:o:microsoft:windows_10_21h2:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.19044.1415**
cpe:2.3:o:microsoft:windows_10_22h2:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.19045.2251**
cpe:2.3:o:microsoft:windows_11_21h2:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.22000.318**
cpe:2.3:o:microsoft:windows_11_22h2:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.22621.674**
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_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) 10.0.14393.4470**
cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.17763.2029**
cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (excluding) 10.0.20348.230**

🐞 **cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*** Show Matching CPE(s)▾	**Up to (excluding) 10.0.19042.1083**

🐞 Denotes Vulnerable Software

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

Change History

9 change records found show changes

QUICK INFO

CVE Dictionary Entry:

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

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