



## Microsoft Patch Tuesday

April 12, 2023

### Executive Summary

Microsoft released patches for 114 vulnerabilities this month, including seven critical and one exploited. The exploited vulnerability, [CVE-2023-28252](#), is an Elevation of Privilege affecting the Windows Common Log File System Driver. With a CVSS score of 7.8, successful exploitation grants SYSTEM privileges. Critical vulnerabilities include [CVE-2023-21554](#), a Remote Code Execution (RCE) vulnerability in Microsoft Message Queuing (MSMQ), with a CVSS score of 9.8. Attackers can send malicious MSMQ packets, leading to RCE on systems with MSMQ service enabled and TCP port 1801 listening. [CVE-2023-28231](#), another critical RCE vulnerability with a CVSS score of 8.8, affects the DHCP Server Service. Authenticated attackers must make a specially crafted RPC call to exploit this vulnerability and gain access to the restricted network. The number of vulnerabilities in each category is listed below.

- 21 Elevation of Privilege
- 7 Security Feature Bypass
- 44 Remote Code Execution (RCE)
- 10 Information Disclosure
- 9 Denial of Service (DoS)
- 7 Spoofing

### Featured Critical Vulnerabilities

The seven (7) critical vulnerabilities listed in April's Patch Tuesday security update are listed below.

<b>DHCP Server Service</b> <a href="#">CVE-2023-28231</a>	<b>Layer 2 Tunneling Protocol</b> <a href="#">CVE-2023-28219</a> <a href="#">CVE-2023-28220</a>	<b>Microsoft Message Queuing</b> <a href="#">CVE-2023-21554</a>
<b>Raw Image Extension</b> <a href="#">CVE-2023-28291</a>	<b>Windows Point-to-Point Tunneling</b> <a href="#">CVE-2023-28232</a>	<b>Windows Pragmatic General Multicast (PGM)</b> <a href="#">CVE-2023-28250</a>

### Safeguards/Recommendations

Organizations should ensure that all systems, software, data, and device settings are backed up prior to performing updates. Users can regularly monitor the "Check for Updates" in their Windows device setting to ensure systems are up-to-date with the latest security patches.

### References

- <https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr>
- <https://msrc.microsoft.com/update-guide/vulnerability>