Multiple Security Updates Affecting TCP/IP: CVE-2021-24074, CVE-2021-24094, and CVE-2021-24086

msrc-blog.microsoft.com/2021/02/09/multiple-security-updates-affecting-tcp-ip/

Today Microsoft released a set of fixes affecting Windows TCP/IP implementation that include two Critical Remote Code Execution (RCE) vulnerabilities (CVE-2021-24074, CVE-2021-24094) and an Important Denial of Service (DoS) vulnerability (CVE-2021-24086). The two RCE vulnerabilities are complex which make it difficult to create functional exploits, so they are not likely in the short term. We believe attackers will be able to create DoS exploits much more quickly and expect all three issues might be exploited with a DoS attack shortly after release. Thus, we recommend customers move quickly to apply Windows security updates this month.

The DoS exploits for these CVEs would allow a remote attacker to cause a stop error. Customers might receive a blue screen on any Windows system that is directly exposed to the internet with minimal network traffic.

It is essential that customers apply Windows updates to address these vulnerabilities as soon as possible. If applying the update quickly is not practical, workarounds are detailed in the CVEs that do not require restarting a server. These three vulnerabilities are unique and require separate workarounds depending on the exposure of an affected system; however, they can be thought of in terms of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) solutions.

The IPv4 workaround simply requires further hardening against the use of Source Routing, which is disallowed in Windows default state. This workaround is documented in CVE-2021-24074 and can be applied through Group Policy or by running a NETSH command that does not require a reboot. The IPv6 workarounds are documented in CVE-2021-24094 and CVE-2021-24086, and require blocking IPv6 fragments, which may negatively impact services with dependencies on IPv6.

Note: IPv4 Source Routing requests and IPv6 fragments can be blocked on an edge device, such as a load balancer or a firewall. This option can be used to mitigate systems with high-risk exposure and then allow the systems to be patched following their standard cadence.

These vulnerabilities were discovered by Microsoft as part of our continual focus on strengthening the security of our products. At this time, we have no evidence that these vulnerabilities were known to any third party. These vulnerabilities result from a flaw in Microsoft's implementation of TCP/IP and affect all Windows versions. Non-Microsoft implementations are not affected.

It is important that affected systems are patched as quickly as possible because of the elevated risk associated with these vulnerabilities, and downloads for these can be found in the Microsoft Security Update Guide. Customers who have automatic updates enabled are automatically protected from these vulnerabilities.