Boston Scientific
Advancing science for life™

MICROSOFT: MULTIPLE SECURITY UPDATES AFFECTING TCP/IP

Boston Scientific is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring the February 9, 2021 announcement of three TCP/IP security vulnerabilities that impact computers running Windows client and server versions starting with Windows 7 and higher. Two vulnerabilities are Remote Code Execution (RCE) vulnerabilities identified in the Windows TCP/IP implementation. The other vulnerability may cause denial of service.

Our global product cybersecurity team is in the process of assessing Boston Scientific products that use the affected Microsoft Window 7 and higher operating systems for any potential vulnerabilities. As we complete this analysis, we will provide an update to this bulletin.

Microsoft has released a set of fixes affecting Windows TCP/IP implementation that includes two RCE vulnerabilities (CVE-2021-24074, CVE-2021-24094) and an Important Denial of Service (DoS) vulnerability (CVE-2021-24086). According to Microsoft, of the three vulnerabilities, the CVE-2021-24086 flaw is most likely to be exploited for orchestration of denial-of-service attacks that cause a STOP error with a Blue Screen (BSOD) in Windows OS.

For more details on the vulnerabilities, refer to:

- Microsoft: Multiple Security Updates Affecting TCP/IP: CVE-2021-24074, CVE-2021-24094, and CVE-2021-24086
- Windows TCP/IP Remote Code Execution Vulnerability: CVE-2021-24074
- Windows TCP/IP Remote Code Execution Vulnerability: CVE-2021-24094
- Windows TCP/IP Denial of Service Vulnerability: CVE-2021-24086

March 09, 2021 Revision 1