BD FACSCanto™ with BD FACSLink™

Date of Critical or Security Patches: January 2019

Microsoft® & Third-Party Patches

BD has reviewed patches from Microsoft® that have been identified as critical or security related for January 2019. The patches include updates that may adversely affect these products. These patches should not be installed on these BD products.

Customers that maintain patches independent of BD delivery should ensure these actions are performed as the acting responsible entity in order to maintain the correct security posture of the system(s).

Patch Name	Patch Description	Patch ID	Notes
January 8, 2019 Monthly Rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.	KB4480970	Not recommended – See Note 1

Notes

1. The January patches were confirmed to disable SMBv1 file shares created on Windows 7 SP1 x86 (32-bit) operating systems. Such file shares may be used for transferring data between FACSCanto instruments and FACSLink middleware. The FACSLink host PC (Win7 SP1 x64) is not impacted.

Advancing the world of health