OVERVIEW

Biosense Webster, Inc. (BWI) has produced a software update that applies both operating system patches and anti-virus signature updates to increase security protection and close known vulnerabilities in the Microsoft Windows based operating system of the CARTO® 3 System. This update will be applied to CARTO® 3 Systems starting in December 2020, as part of the free-of-charge CARTO® 3 Version 6 SP3 base software version, which is designed to upgrade compatible CARTO® 3 Systems running Version 6 (V6).

BACKGROUND

The affected product, the CARTO® 3 V6 System, is an advanced imaging device that uses electromagnetic technology to create real-time three-dimensional (3D) maps of a patient’s cardiac structures. The system is designed to help electrophysiologists navigate the heart by generating an accurate 3D map, as well as pinpointing the exact location and orientation of catheters in the heart during diagnostic and therapeutic procedures for patients suffering from heart rhythm conditions (cardiac arrhythmias).

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Windows Operating System vulnerabilities are regularly identified and addressed by Microsoft. Microsoft informed the public about these vulnerabilities and fixes through advisories and knowledge base articles (KB #) and downloadable security updates.

CARTO 3 V6 SP 3 includes the following list of security KB articles and associated Common Vulnerabilities and Exposures (CVE). For more details on the KB# and the impacts, severities, details and associated CVEs, please follow the link: https://msrc.microsoft.com/update-guide

Knowledge Base Number (KB#)	Title	CVEs
4019990	Update for the d3dcompiler_47.dll component on Windows Server 2012, Windows 7, and Windows Server 2008 R2.	
4474419	SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008	
4490628	Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1	
4524157	Addresses an intermittent issue with the print spooler service that may cause print jobs to fail. Some apps may close or generate errors, such as the	

	remote procedure call (RPC) error	
4520003	• Addresses an issue in security bulletin CVE-2019-1318 that may cause client or server computers that don’t support Extended Master Secret (EMS) RFC 7627 to have increased connection latency and CPU utilization. This issue occurs while performing full Transport Layer Security (TLS) handshakes from devices that don’t support EMS, especially on servers. EMS support has been available for all the supported versions of Windows since calendar year 2015 and is being incrementally enforced by the installation of the October 8, 2019 and later monthly updates. • Security updates to Windows Authentication, Microsoft JET Database Engine, Windows Kernel, Internet Information Services, and Windows Server.	CVE-2019-1318
4525233	• Provides protections against the Intel® Processor Machine Check Error vulnerability (CVE-2018-12207). Use the registry setting as described in the Guidance KB article. (This registry setting is disabled by default.) • Provides protections against the Intel® Transactional Synchronization Extensions (Intel® TSX) Transaction Asynchronous Abort vulnerability (CVE-2019-11135). Use the registry settings as described in the Windows Client and Windows Server articles. (These registry settings are enabled by default for Windows Client OS editions but disabled by default for Windows Server OS editions.) • Security updates to Windows Input and Composition, Microsoft Graphics Component,	CVE-2018-12207 CVE-2019-11135

	Windows Cryptography, Windows Virtualization, Windows Kernel, Windows Datacenter Networking, and the Microsoft JET Database Engine.	
4530692	Security updates to Windows Input and Composition, Windows Virtualization, Windows Kernel, Windows Peripherals, and Windows Server	
4534310	Security updates to the Microsoft Scripting Engine, Windows Input and Composition, Windows Storage and Filesystems, and Windows Server	
4534314	Security updates to Windows Input and Composition, Windows Storage and Filesystems, and Windows Server.	
4536952	Servicing stack update for Windows 7 SP1 and Server 2008 R2 SP1	
4538483	Extended Security Updates (ESU) Licensing Preparation Package for Windows 7 SP1 and Windows Server 2008 R2 SP1	
4532932	Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2	
4532971	- Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2	
4532945	Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1	
4532960	Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1	