

*****ADVISORY NOTICE*****

DePuy Synthes Distributed Brainlab KICK® CAS System

Awareness for Virus Vulnerability and Software Update Verification

July 18, 2017

Product:

Brainlab's KICK® System is a computer-aided surgical navigation system using optical tracking to assist surgeons during surgical procedures. DePuy Synthes is a distributor of the Brainlab KICK® System.



Potential Issue:

Computers around the world have recently been exploited by ransomware (e.g. WannaCrypt or WannaCry, Petya/NotPetya). The malicious software encrypts local computer files, as well as files on the connected network shared with the infected Windows-based computers. The software locks the affected computers and prevents their use until a fee is paid. The KICK® System may be exposed to this threat if the KICK® System is connected through its Ethernet port to a network.

As of the date of publication of this bulletin there are no reported events of ransomware impacting KICK® Systems.

Recommended Actions:

These ransomware attacks have identified the importance of verifying that the most current operating system patches have been installed on the KICK® System. Customers should:

- Verify that the Microsoft patch identified as MS17-010 (KB4012212 or KB4012215) has been installed on the KICK® System. Customers should contact Brainlab technical support for assistance.
- Backup medical records stored on the KICK® System. Brainlab recommends customers refer to the User Guide for backing up medical records.

If customers are concerned a KICK® System has been impacted by a cyber-attack, please immediately disconnect the system from the network and contact Brainlab technical support.

Europe, Africa, Asia and Australia

Phone: +49 89 99 15 68 1044

Fax: +49 89 99 15 68 5811

Mail: support@brainlab.com

United States, Canada, Central and South America

Phone: +1 (800) 597-5911

Fax: +1 (708) 409-1619

Mail: us.support@brainlab.com

FAQ

Why is DePuy Synthes distributing this advisory for a Brainlab product?

During the past few months, malicious ransomware software has been spreading on computers worldwide. This ransomware encrypts local files as well as files on connected network shares of infected Windows computers. Affected users are requested to pay a certain amount and to have their data unlocked. This is a global issue and not an isolated event affecting Brainlab devices. DePuy Synthes is a distributor of the Brainlab KICK® System.

What does this mean for KICK® customers?

As Brainlab products are operated with Microsoft Windows, they can in principle also be attacked by ransomware. However, only those systems that have not been updated with the latest Microsoft patches are vulnerable.

The vulnerability associated with ransomware has mainly been exploited on Windows systems unless they have been patched to the latest level.

Brainlab advises customers to always patch Brainlab systems as soon as patches become available. Refer to the Antivirus and Windows Update instructions in the User Guide provided with your KICK® System.

What can you do?

Verify the correct software updates/patches have been installed on your KICK® System, and install them if they are not current. Should you be affected by the ransomware attack, collect as much relevant information as possible and provide your input and questions to the Brainlab Hotline.

Is only Brainlab affected?

This is a global issue and not an isolated event affecting Brainlab devices.