STORZ
KARL STORZ—ENDOSKOPE

ENDOSCOPES FOR MEDICINE AND TECHNICAL SCIENCE
INSTRUMENTS FOR OTO-RHINO-LARYNGOLOGY

KARL STORZ GmbH & Co. KG • P. O. Box 230 • D-78503 Tuttlingen

THE GLOBAL COMPACT
WE SUPPORT

To whom it may concern

Date
5/31/2017

Information regarding malicious software (Malware)

Dear Sir or Madam,

In light of recent cyber-attacks reported by various media outlets, malicious software has been put into circulation that could have damaging effects on computer systems. To minimize your risk of exposure, we recommend adhering to the Malware General Preventative Guidelines listed below. In addition, there is a table in this document with current protection and specific recommendations for all the major Karl Storz systems as well as details on Whitelisting SE46, Security update MS17-010 and network recommendations to minimize any malicious threats.

Therefore we would like to recommend the following:

- Never open unverified file attachments, regardless of whether they appear to be harmless files like images, documents or other files. If you are unsure, check with the sender.
- Never click on links in unsolicited emails that have been sent to you. They could route you to infected websites and could result in an unnoticed download.
- On social networks, do not indiscriminately click on sensational videos or other notifications—even if they were recommended by friends.
- Regularly install security updates for your operating system provided by the manufacturer and update programs you have installed (e.g. Browser, Flash Player, Adobe Reader), ideally using the "Automatic Updates" function.
- Use an anti-virus program and update it regularly.
- Do not use the Internet when in Administrator mode. Create a "User" with standard user rights and use it for surfing the Internet.
- Backup your data regularly to an external medium to keep data loss to a minimum.

Office Address:
KARL STORZ GmbH & Co. KG
Mittelstraße 8
D-78532 Tuttlingen

Phone: +49 (0)7461 708-0
Fax: +49 (0)7461 708-105
E-Mail: info@karlstorz.de
Web: www.karlstorz.com
WEEE Reg. No: DE 74465858

Kommanditgesellschaft:
KARL STORZ GmbH & Co. KG
Registered in Tuttlingen
Commercial Register: Stuttgart HRA 450442
VAT DE 142931059

Unlimited Partner:
KARL STORZ-Verwaltungsgesellschaft mbH
Registered in Tuttlingen
Commercial Register: Stuttgart HRB 450225
Managing Partner: Sybill Storz Dr. h.c. mult.

Bank accounts:
Volksbank Donau-Neckar eG Tuttlingen (BLZ 643 901 30)
Acc. No. 772 003, SWIFT: GENO DES1TUT
IBAN: DE97 6439 0130 0000 7720 03

Commerzbank AG Tuttlingen (BLZ 643 800 11)
Acc. No. 2 713 305 00, SWIFT: DRES DE FF 643
IBAN: DE69 6438 0011 0271 3305 00

Kreissparkasse Tuttlingen (BLZ 643 500 70)
Acc. No. 1322 SWIFT: SOLA DES 1 TUT
IBAN: DE79 6435 0070 0000 0013 22

Deutsche Bank AG Tuttlingen (BLZ 653 700 75)
Acc. No. 211 639 000 SWIFT: DEUT DESS653
IBAN: DE09 6537 0075 0211 6390 00

93 703 21

If you have questions please contact us using the contact address at our homepage: www.karlstorz.com

Description:
As of May 25, 2017, the “WannaCry” is a ransomware which encrypts user’s files. This ransomware can spread in two methods: executable and through network file shares. To spread through an executable requires a user to run a program or open a document which has the ransomware embedded. To become infected through the file share, no user interaction is required, but the computer must a) have file sharing enabled (server), b) support the SMBv1 protocol.

In addition to the above recommendations, we would like to provide the following technical information on our products:

System/Version	Operating System	Protected	Recommendations
KARL STORZ OR1 FUSION®, all versions	Windows 7 Professional for Embedded Systems	Protected against “WannaCrypt”-Ransomware with SE46 Whitelist agent which prevents the execution of ransomware.	1. Install security update MS17-010. 2. Network mitigation.
AIDA™, all versions of WD 200 and WD 250	Windows 7 Professional for Embedded Systems	Protected against “WannaCrypt”-Ransomware with SE46 Whitelist agent which prevents the execution of ransomware.	1. Install security update MS17-010. 2. Network mitigation.
AIDA™ compact NEO 3.2	Windows XP Professional for Embedded Systems	Protected against “WannaCrypt”-Ransomware with SE46 Whitelist agent which prevents the execution of ransomware.	1. Install security update MS17-010. 2. Network mitigation.
AIDA™ compact NEO 3.0 AIDA™ compact NEO 3.1	Windows XP Professional for Embedded Systems	Protected against “WannaCrypt”-Ransomware with default firewall rule block “file and printer sharing” is active, which means the ports 139, 445, 137 and 138 are blocked.	1. Update with AIDA compact NEO 3.2. 2. Install security update MS17-010. 3. Network mitigation.
AIDA™ compact II 2.3 AIDA™ compact II 2.4	Windows XP Professional for Embedded Systems	Protected against “WannaCrypt”-Ransomware with default firewall rule block “file and printer sharing” is active, which means the ports 139, 445, 137 and 138 are blocked).	1. Install security update MS17-010. 2. Network mitigation.
AIDA™ compact II 2.0 AIDA™ compact II 2.1 AIDA™ compact II 2.2	Windows XP Embedded with SP2	Protected against “WannaCrypt”-Ransomware with default firewall rule block “file and printer sharing” is active, which means the ports 139, 445, 137 and 138 are blocked).	1. Network mitigation.

AIDA™ mini	Windows CE	Operating system is not affected.	
AIDA™ Advanced Reporter, all versions	Client: Windows XP / Vista / 7 / 8 / 10 Server: Windows Server 2003 / 2008 / 2012 R2	Not affected with regular OS patch management as recommended.	1. Install security update MS17-010.
SCENARA® .connect, all versions of WS 100-C	Windows Server 2012 R2	Not affected with regular OS patch management as recommended.	1. Install security update MS17-010.
SCENARA® . store, all versions of WS 100-S	Windows Server 2012 R2	Not affected with regular OS patch management as recommended.	1. Install security update MS17-010.
SCB control NEO software, 200900 01-41 or higher	Windows XP Embedded SP3	Not affected, because no connection to the Hospital Network is required. If connected to an AIDA compact NEO, FUSION or AIDA WD200/250 a dedicated point-to-point connection is used, which is separated from the Hospital Network.	1. Verify that a dedicated network connection is used as described in the instructions for use "Installation manual" in the chapter "Network connection".
SCB control NEO software, 200900 01-46 or higher	Windows XP Embedded SP3	Not affected, because no connection to the Hospital Network is required. If connected to an AIDA compact NEO, FUSION or AIDA WD200/250 a dedicated point-to-point connection is used, which is separated from the Hospital Network. When a device such as AUTOCON III 400 or BOWA ARC 400 is also connected, the communication takes place on a from the Hospital Network separated network (via a separated network switch).	1. Verify that a dedicated network connection is used as described in the instructions for use "SCB control NEO System Release 4x" in the chapter "System variants".
AIDA HD Connect, version 070111-014BE 2.0.0.3603	Windowx 7 Embedded	Not affected provided firewall remains enabled (default) and when joined to Active Directory no group policy that allows SMB (port 445) is applied. Apply mitigations as recommended.	1. Network Mitigations 2. Disable SMB

Streamconnect NEO, version 3.0.3 and 4.0.0	Windows Server 2012 R2	Apply mitigations as recommended.	1. Network Mitigations 2. Install security update MS17-010. 3. Disable SMB
Overview NEO, version 1.0.2	Windows 7	Not affected, because no connection to the Hospital Network is required.	1. Verify that a dedicated, closed network is used as described in the instructions for use. 2. Disable SMB 3. Disable or block USB

Whitelisting SE46

This Application Whitelist solution ensures that only trusted software and hardware is allowed to run on a mission-critical machines and computer workstations. This agent using the principal of "Deny by Default" and reject any file that is not part of an authorized application as undesirable and never permits it to start. The result is that any virus or unauthorized software is completely blocked and therefore can never pose a threat. Since 2012 KARL STORZ AIDA® and KARL STORZ OR1 FUSION® systems are installed with an Application Whitelist solution and had never a fault indication regarding ransomware. The Whitelist approach are also protecting for unknown "zero-day exploit".

Security update MS17-010

Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017. Apply Microsoft updates in a test environment first to confirm functionality of the system. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003 operating systems on May 13, 2017.
For KARL STORZ OR1 FUSION®, KARL STORZ AIDA® (WD 200 and WD 250), and AIDA™ compact NEO 3.2 with an Application Whitelist solution you have to temporarily activate the service mode of the Local Whitelist Manager to install the security update.

Network Mitigation

1. Disconnect Network: If you not use network functionality you can disconnect the unit from the network prevents an infection via the network interface and the file share infection vector.
2. Restricted VLAN: It is strongly recommended to use a restricted VLAN and allow only outbound access to those systems which are necessary (Active Directory, network file shares, etc.). No access to the internet is required, nor recommended.

Disable SMB

3. If you don't use SMB protocol disable SMBv1 and SMB server mode. This can be done via group policy and should apply to the specific device OU in which the unit is contained. It can also be done by executing the following commands from command line when logged in as administrator:

   a) Disable SMBv1: reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v SMB1 /t REG_DWORD /d 0 /f

b) Disable ADMIN shares:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v AutoShareServer /t REG_DWORD /d 0 /f
```

c) Disable ADMIN shares:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v AutoShareWks /t REG_DWORD /d 0 /f
```

4. For Windows Server 2012 R2
   a. Execute the following commands from command line when logged in as administrator. From a powershell, run the following:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

References

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

https://support.microsoft.com/en-us/help/4023262/how-to-verify-that-ms17-010-is-installed

US CERT:

https://www.us-cert.gov/ncas/alerts/TA17-132A

Nexus group:

https://www.nexusgroup.com/blog/save-yourself-from-cyber-attacks/

...

Best regards,

KARL STORZ GmbH & Co. KG

i.V.

Serkan Sezer
Vice President
Global Quality Management, Regulatory Affairs, RSB & Service