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

May 16, 2019 Security Notice CVE 2019-0708

To whom it may concern,

Microsoft (CVE-2019-0708) Remote Desktop Services Remote Code Execution Vulnerability

Dear Sir or Madam,

KARL STORZ is aware of and currently monitoring the Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708). This vulnerability was announced by Microsoft on May 14, 2019. This vulnerability affects any systems that use Remote Desktop Services for Windows XP, Windows 7, Windows 2003 Windows Server 2008 and Windows Server 2008R2.

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using Remote Desktop Protocol (RDP) and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Similar to other worm type malware, exploits to this vulnerability could spread from vulnerable computer to vulnerable computer.

KARL STORZ has had no reports of this vulnerability being exploited on a KARL STORZ product, but is currently working to test and validate the Microsoft patch for KARL STORZ products that use Remote Desktop Services to create a KARL STORZ Security Patch release. Additionally, KARL STORZ recommends to follow Microsoft's mitigations and workarounds for systems that use Remote Desktop Services and communicate with the RDP server for Windows XP, Windows 7, Windows 2003, Windows Server 2008 and Windows Server 2008 R2:

Mitigation

- Disable Remote Desktop Services if they are not required.

Workaround

- Enable Network Level Authentication (NLA) on systems running editions of Windows XP, Windows 7, Windows 2003, Windows Server 2008 and Windows Server 2008 R2
- Block TCP port 3389 at the enterprise perimeter firewall

KARL STORZ
Endoscopy-America, Inc.
2151 E. Grand Avenue
El Segundo, California 90245-5017
Phone 424 218 8100
Toll Free 800 421 0837
Fax 800 321 1304

Employ Good Network Hygiene Practices

- Ensure data has been backed up and stored according to your individual processes and disaster recovery procedures
- Execute updates to malware protection, where available

Note: These mitigations, workarounds and hygiene recommendations provide protection against ‘wormable’ malware or advanced malware threats that could exploit the vulnerability, as NLA requires authentication before the vulnerability can be triggered. However, affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

Customers that maintain Virtual Machine (VM) system patches independent of KARL STORZ patch release should ensure these actions are performed to maintain the correct security posture of the system(s).

- For more information and instructions on how to apply the Microsoft security patch, please follow the link below:
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

KARL STORZ will provide a follow-up communication upon completion of our testing and verification of the Microsoft patch on any effected systems. If you have questions please contact us using the contact address: robert.haack@karlstorz.com.