Updated: 5/17/2109

FAQs:

1. **What Keysight products are vulnerable to the recent Microsoft vulnerability (CVE-2019-0708)?**

   Any Keysight product based on the Windows XP or Windows 7 operating system is potentially vulnerable. Products using Windows 10, Windows CE and Linux based operating systems are not affected.

2. **What is the risk of the vulnerability?**

   As of May 17, 2019, Keysight is unaware of any active exploit of this vulnerability. However, future malware could use the vulnerability to spread to other connected devices. Because of this potential risk, Keysight recommends customers be proactive to address this vulnerability.

3. **How can I protect my Keysight products based on Windows XP or Windows 7 operating systems from this vulnerability?**
   - **Review the Microsoft guidance for this vulnerability** – Available through Microsoft's Prevent a worm by updating Remote Desktop Services page.
   - **Update to the latest Microsoft security patches**
     - Updates for Windows 7 products can be performed using the Windows Update capability found on the product, or by downloading the appropriate Windows 7 update directly from the Windows 7 Microsoft Update Catalog page and installing the patch manually.
     - For Windows XP products, the Windows XP update must be downloaded and installed manually from the Windows XP Microsoft Update Catalog page. PLEASE NOTE: Windows XP products must be running Windows XP Service Pack 3 (SP3) to utilize the published Microsoft updates. If the product is not running SP3 they will need to install it – see Windows XP SP3 Microsoft Update Catalog page.
   - **Consider alternative mitigation as outlined by Microsoft** – See Microsoft's Remote Desktop Services Remote Code Execution Vulnerability page. Though these mitigations may help reduce the risk of exploit, Microsoft strongly recommends that the updates for this vulnerability be installed as soon as possible even if the workarounds are left in place.

4. **How else can Keysight products be protected from a virus or malware?**

   For Window 7 based products:

   Keysight recommends enabling automatic update notifications, which allows a message to be presented on the instrument as critical security patches become available. You may further elect to enable automatic acceptance of such patches or not. In some cases, such as production uses, it may not be viable to enable these notifications. Therefore, you should consider enabling notifications based on individual business risks and user discretion. Instructions from Microsoft can be found on the Windows Update FAQ page.

For Windows XP based products:

Since Windows XP is no longer officially supported by Microsoft, there is no Windows Update service. In rare situations, like this one, Microsoft may provide security updates for critical vulnerabilities that can be installed manually. Keysight recommends customers evaluate the security risks of these products based on how they are used in their environment and consider upgrading to a supported operating system (or to a newer product) if needed.

5. **Should Anti-Virus scans be run on Keysight equipment?**

   See the FAQ answer in the Keysight Computer Virus Control Program document.