Service Bulletin, Bluekeep Vulnerability

Table of Contents:

1. SCOPE

This service bulletin describes the procedure for installing security updates to the ATS instruments using the Windows 7 and older operating systems.

2. PRODUCTS AFFECTED

All ATS Gen4+ and Gen5 instruments using the Windows 7 OS.

3. SUMMARY OF PROBLEM

An exploit called Bluekeep, or CVE-2019-0708, takes advantage of a vulnerability in the built-in remote desktop functionality for Windows 7. The ATS Gen4+ and Gen5 models are affected by this exploit.

Customers can install security updates to protect their system from this vulnerability. Field service engineers are not required to go onsite to install the updates. Customers can be directed to the EDC Biosystems website for information: https://www.edcbiosystems.com/company/news-events.

4. DETAILS OF SECURITY UPDATE

Customers can install the following patches on their ATS instruments:

Operating System	Patch
Windows 7	KB4499175

The patch has been evaluated and validated by EDC Biosystems on a Gen 5 Windows 7 instrument. Customers can follow the steps in the bulletin to install the patch.

EDC Biosystems
Fremont, CA 94538

Service Bulletin, Bluekeep Vulnerability

Bulletin. No. 51454 rev A   Released: June 24, 2019

__NOTE!__ Customers should only install the patch as a standalone update, and not install the patch through the Windows Update. A standalone package can be downloaded here:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4499175

5. SECURITY UPDATE INSTALLATION PROCEDURE

1. Turn on the power to the ATS instrument and allow the PC to boot.
2. Launch the ATS AutoRun software.
3. Allow the instrument to complete the homing sequence.
4. Verify the instrument homes properly.
5. Close the ATS AutoRun software.
6. Install the CVE-2019-0708 patch.
7. Reboot the ATS.
8. Launch the ATS AutoRun software and allow the instrument to complete the homing sequence.
9. Verify the instrument homes properly.