



July 09, 2019

AutoMate 2500 MICROSOFT REMOTE CODE EXECUTION VULNERABILITY IN REMOTE DESKTOP SERVICES (CVE-2019-0708)

Dear Valued Customer,

At Beckman Coulter, we develop technologies to advance and optimize the laboratory. To achieve this, we uphold core values that define our responsibility to those we serve. Among them: an unwavering commitment to the safety and security of patients and laboratory personnel. Therefore, we believe in continuously improving to address the ever-evolving privacy and cybersecurity landscape.

On May 15th, 2019, Microsoft released a patch for a critical Remote Code Execution vulnerability in Remote Desktop Services (CVE-2019-0708). This vulnerability can be exploited remotely without authentication on systems that use Remote Desktop Services for Windows XP, Windows 7, Windows Server 2003 and Windows Server 2008 operating systems. Installations running Windows 10 are not affected.

In response to potential threats to cybersecurity like this one, Beckman Coulter has formed a global product security team chartered to assess providing security updates and patches as a non-reportable event, but we still have an obligation to validate these updates to ensure that there is no impact to essential clinical performance of our products. Please visit <https://www.beckmancoulter.com/en/about-beckman-coulter/product-security/product-security-updates> for latest information on our response to cybersecurity threats.

To address this recent vulnerability, we have released the following Microsoft patches that we have validated and are available for download from <https://www.beckmancoulter.com/wsrportal/page/softwareDownloadSearch>.

Steps to Download:

- 1) From the home page, if you have not already done so, please click on *Register* to enter your information.
- 2) If you have already registered, please proceed to click on *Log In* and select *Software Downloads* from the drop down menu.
- 3) From there, please make the following selections in the Drop-Down entries for each field:

The screenshot shows a web form titled "Software Download" with a tabbed interface. The active tab is "Search By Product". Below the tab, there are five dropdown menus: "Market Segment*" (set to "Diagnostics"), "Product Line*" (set to "Automation"), "Product Series" (set to "Automate 2500 Family"), "Product" (set to "Automate 2500 Family"), and "Software Name" (set to "All Software"). There is also a "Language" dropdown menu set to "English". A "Search" button is located below the dropdowns. At the bottom of the form, there are two additional search options: "Search By Software Name" and "Search By Item/REF Number". A small asterisk note indicates that fields with an asterisk are required.

- 4) You will then be taken to the list of following patches. Please download the appropriate one(s) for your system to the media of your choice.

Date	OS	Patch / KB	File size	Notes
June 20, 2019	Windows XP with SP3	KB4500331	526 KB	
June 20, 2019	Windows 7 32 bits	KB4499175	72.3 MB	

- 5) Follow the associated instructions to install the patch on your AutoMate 2500 system.
6) After installation completes, then your AutoMate 2500 system has been updated with this patch.

Should you require further assistance, please contact your Beckman Coulter representative.

Thank you for your continued loyalty!

Beckman Coulter Inc.

© 2019 Beckman Coulter. All rights reserved. Beckman Coulter, the stylized logo, and the Beckman Coulter product and service marks mentioned herein are trademarks or registered trademarks of Beckman Coulter, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

Beckman Coulter – June xx, 2019 Customer Letter for AutoMate 2500 and Remote Code Execution Vulnerability in Remote Desktop Services (CVE-2019-0708)