Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

Waters Informatics
Customer Guidance for WannaCrypt Attacks

What is it?

In response to the "WannaCrypt' attack, Microsoft has published information relating to the necessary updates required to close the vulnerability. Please see Microsoft Bulletin MS17-010 for more information. This applies to currently supported Windows operating systems as well as those platforms that are currently only available under Custom Support (Windows XP, Windows 8, and Windows Server 2003). This update was created for the previously mentioned Custom Supported platforms on May 12, 2017. An update was available in March 2017 for currently supported platforms (Windows 7, Windows Vista, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2).

How does this Affect Waters Informatics Products?

Waters has reviewed this information, and based on the affected areas have determined that applying the Windows Update provided **will not negatively affect** its Empower CDS or NuGenesis LMS products. Microsoft has provided this update for supported platforms in March 2017. Many of our customers have successfully applied this update without any issue. Waters has performed initial testing of our applications with this update applied, and have not encountered issues related to this update.

The Windows update is a roll-up that supersedes many earlier updates and contains updates to Time Zones that have been previously identified as problematic for our UNIFI software. While the particular solution to the identified vulnerability is not an issue, the delivery of this solution as a bundled update is. Applying this Windows update to UNIFI 1.5.x, 1.6.x, 1.7.x, 1.8.0 and 1.8.1 can cause issues with the software and its operation. These issues are addressed in UNIFI 1.8.2 and later.. At this time, Waters recommends updating the UNIFI software to version 1.8.2 to properly protect your system and maintain system operability or remove the Windows update from your system to allow UNIFI to function.

Waters Current Policy on Windows Updates

Waters recommends regularly applying Windows updates as available to keep your systems secure. Waters policy is not to test every Microsoft Update or security patch that may be released. For those Microsoft Updates that Waters determines to be critical to our software applications, Waters will perform a set of regression tests. This subset of testing will only be performed on the latest version of each software package.

Additional Information

Microsoft Customer Guidance for WannaCrypt attacks

Microsoft Bulletin MS17-010

Waters Corporation
34 Maple Street, Milford, MA 01757 USA **[T]** 508.478.2000 **[T]** 1.800.525.4752 **[F]** 508.872.1990
www.waters.com