PRODUCT SECURITY ADVISORY

22 May 2019

Title/Security Advisory ID: Microsoft® Remote Desktop Services Remote Code Execution Vulnerability (a.k.a. “BlueKeep”).

Overview: Microsoft discovered a vulnerability in its Remote Desktop service that is included in most versions of a wide variety of its operating systems. Although this vulnerability is not associated with any specific Johnson Controls application, it does impact the computer environments that can host those applications.

Impact: In certain circumstances, this vulnerability could be used to gain unauthorized remote access to a system.

Solution: Microsoft has released a product update that patches this security issue.
The update addresses this vulnerability by correcting how Remote Desktop Services handles connection requests.

Recommended Actions. Customers are advised to execute the following steps:

1. Promptly apply Microsoft security patches to your environments. See information below for specifically impacted Microsoft products.
2. If systems are accessed remotely, make certain that the remote connection is secure using a virtual private network (VPN) tunnel with two-factor authentication or equivalent secure remote access method.

In addition to the recommendations above, it is important to continue the best practice of applying updates to all applications and operating systems on a regular basis including updates to Johnson Controls applications.

Johnson Controls Product Support:
For product specific questions, including how to identify if your Johnson Controls product needs to be patched, customers should leverage their normal product sales and support contacts. As always, you can reach the Johnson Controls Cyber Solutions team at productsecurity@jci.com

Affected Microsoft Products. The following versions of Microsoft Windows® operating systems and servers are affected by the BlueKeep issue:

Vulnerable in-support systems include Windows 7 operating system, Windows Server® 2008 R2, and Windows Server 2008 systems.

Out-of-support but affected operating systems include Windows Server 2003 and Windows XP® operating systems.

For a more detailed list from Microsoft, see the following:

Microsoft list of affected, mainstream supported products:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708#ID0EKIAC

Microsoft list of affected but non-supported products:
https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

Additional Resources:
Downloads for in-support versions of Windows operating systems and servers can be found in the Microsoft Security Update Guide: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

To learn more about Johnson Controls approach to cybersecurity, please visit us at
https://www.johnsoncontrols.com/cyber-solutions

U.S. Department of Homeland Security ICS Security Guidance:
https://ics-cert.us-cert.gov/Recommended-Practices

General media article on the topic:
https://securityaffairs.co/wordpress/85569/security/windows-rdp-flaw.html

Johnson Controls