Baxter Product Security Bulletin

Microsoft Security Advisory for CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability"

Publication Date: May 16, 2019
Last Update: August 08, 2019
Version: V2.0

SUMMARY
As part of our Product Security program, Baxter has reviewed the Microsoft security advisory for CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability" to assess the associated potential risks. This vulnerability affects any systems that use Remote Desktop Services for Windows XP, Windows 7, Windows Server 2003, and Windows Server 2008. For a more detailed description of this vulnerability, it is recommended that customers view the information provided by Microsoft. **To date, Baxter has not received any reports of these vulnerabilities impacting clinical use of any ExactaMix product.**

VULNERABILITY DESCRIPTION
A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using Remote Desktop Protocol (RDP) and sends specially crafted requests. Microsoft released patches for all affected operating systems, including those currently out of support.

RECOMMENDATIONS
For facilities that have installed Baxter applications on customer-owned windows machines, please follow the guidance recommended by Microsoft, where applicable, to these systems.

The following Baxter products run on an operating system which has been determined by Microsoft to be susceptible to the Remote Desktop Protocol (RDP) vulnerability.

- ExactaMix (EM2400) v1.10/v1.11
- ExactaMix (EM1200) v1.1/1.2

These products are designed with security controls that do not allow users to connect remotely to the product using RDP, reducing exposure to the vulnerability identified by Microsoft and protecting against remote code execution.

Nonetheless, Baxter recommends customers upgrade to the new software version for the ExactaMix EM1200 Compounder (v1.4) and ExactaMix EM2400 Compounder (v1.13) that features the Microsoft Windows 10 operating system, which is not susceptible to CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability." To schedule this upgrade or for questions regarding installation and configuration of ExactaMix, call your Baxter US technical support center at 1-800-678-2292, or contact your local technical support call center.

Baxter also recommends the following mitigations:

- Ensure the updates Microsoft provided have been applied, where applicable, to customer-owned windows machines in your general network, the ExactaMix file share, and machines on which your order management software is installed.
- Follow the segmentation and all other recommendations described in the ExactaMix Cybersecurity Guide, which can be requested from productsecurity@baxter.com
- Ensure your network firewall blocks port 3389 traffic.

CONCLUSION

As noted, to date, Baxter has not received any reports of these vulnerabilities impacting clinical use of any ExactaMix product. If you observe any symptom of this vulnerability, disconnect your system and contact your service representative immediately. Please contact the Baxter Product Security team at productsecurity@baxter.com if you have any additional questions. As new information becomes available, Baxter will assess for any potential impact on its products and update this security bulletin.

ADDITIONAL RESOURCES

NIST National Vulnerability Database | https://nvd.nist.gov/vuln/detail/CVE-2019-0708

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Customer guidance for CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: May 14, 2019 https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708