Baxter Product Security Bulletin

CISA alert AA20-014A “Critical Vulnerabilities in Microsoft Windows Operating Systems”

Publication Date: March 17, 2020
Last Update: March 17, 2020
Version: V1.0

SUMMARY

As part of our Product Security program, Baxter has reviewed the CISA advisory for AA20-014A[1] “Critical Vulnerabilities in Microsoft Windows Operating Systems” to assess the associated potential risks. The vulnerabilities affect any Windows 10 systems using Elliptical Curve Cryptography (CVE-2020-0601), any Windows Server 2012 or newer systems using Windows Remote Desktop Gateway (CVE-2020-0609/CVE-2020-0610), and any Windows 7 or newer systems using Windows Remote Desktop Client (CVE-2020-0611). For a more detailed description of these vulnerabilities, it is recommended that customers view the information provided by Microsoft.

IMPACTING VULNERABILITY DESCRIPTION

Baxter products have been evaluated and the ExactaMix products specified below were determined to be susceptible to one of the vulnerabilities - CVE-2020-0611[2], Remote Desktop Client Remote Code Execution Vulnerability. This is a remote code execution vulnerability that exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. The vulnerability requires connection to a malicious server via social engineering, Domain Name Server (DNS) poisoning, a man-in the-middle attack, or an attacker compromising a legitimate server.

AFFECTED PRODUCTS

The following Baxter products run on Windows operating systems that are impacted by the CVE-2020-0611 vulnerability:

- ExactaMix v1.4/v1.5 (EM1200)
- ExactaMix v1.13/v1.14 (EM2400)

RESPONSE

To date, Baxter has not received any reports of this vulnerability impacting clinical use of any Baxter product. Baxter continues to monitor the available information regarding this issue and assess for any potential impact on its products. 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 update this security bulletin.

RECOMMENDATIONS

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

As noted above, ExactaMix v1.4/v1.5/v1.13/v1.14 systems run on Windows operating systems which have been determined to be susceptible to the CVE-2020-0611 vulnerability.

Baxter recommends the following compensating controls for all ExactaMix customers:

- The ExactaMix compounder should be segmented from the main customer network, and have all non-required communication blocked via firewall and ACL configuration.
- The customer should follow standard guidance to ensure security patches are up to date on their main network.
- The customer should follow proper backup and storage procedures to maintain the integrity of data utilized with the ExactaMix compounder.

Baxter separately provided an ExactaMix Cybersecurity Guide instructing customers on good cybersecurity practices relevant to the use of the ExactaMix product. The guide can be requested from productsecurity@baxter.com.

CONCLUSION

If you observe any symptom of these vulnerabilities, 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

Please see the following additional resources:

1. https://www.us-cert.gov/ncas/alerts/aa20-014a
2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611