Product Security Bulletin

Title: ExactaMix Advisory ICSMA-20-170-01
Publication Date: June 18, 2020

Updated: June 18, 2020

In support of our mission of saving and sustaining lives, Baxter takes product security seriously. Baxter has reviewed the ExactaMix product line for cybersecurity related vulnerabilities and is voluntarily disclosing the following vulnerabilities per our responsible disclosure process.

Vulnerability Summary

The following vulnerabilities were identified in the ExactaMix EM2400 V1.10, V1.11, V1.13, V1.14 and ExactaMix EM1200 V1.1, V1.2, V1.4, V1.5 systems. There have been no reports of the following vulnerabilities being exploited.

CVE-2020-12016 - A threat actor with network access to ExactaMix compounder could log into the ExactaMix operating system using hardcoded Administrative credentials, allowing unauthorized access to system resources, including access to execute software or to view/update files, directories, or system configuration. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.

Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2, 1.4, 1.5
- ExactaMix 2400 versions 1.10, 1.11, 1.13, 1.14

CVE-2020-12012 – A threat actor with physical access to ExactaMix compounders could log into the ExactaMix Application using hardcoded Administrative credentials, allowing unauthorized access to view or update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.

Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2, 1.4
- ExactaMix 2400 versions 1.10, 1.11, 1.13

CVE-2020-12008 – A threat actor with access to the network the File Share and ExactaMix resides on could observe prescription files sent between the File Share system and ExactaMix. ExactaMix uses un-encrypted (clear-text) protocol to retrieve clear-text files from its File Share. The un-encrypted communication is used to transfer prescription files (PAT files). The prescription file contains PHI.

Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2
- ExactaMix 2400 versions 1.10, 1.11

CVE-2020-12032 – ExactaMix Systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view sensitive data including PHI.

Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2
- ExactaMix 2400 versions 1.10, 1.11

CVE-2020-12024 – ExactaMix Systems do not restrict access to the USB from an unauthorized user. This may allow an attacker with physical access to the system unauthorized access to the hard drive by booting a live USB OS. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.

Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2, 1.4, 1.5
- ExactaMix 2400 versions 1.10, 1.11, 1.13, 1.14

CVE-2020-12020 – A threat actor that does not have privileged operating system access still has access to the startup script. This may allow an attacker with non-privileged access to alter the startup script and delete the ExactaMix application, making the system unavailable for use.

Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2, 1.4
- ExactaMix 2400 versions 1.10, 1.11, 1.13

CVE-2017-0143 – ExactaMix Systems do not validate or incorrectly validates input via the SMBv1 port that can affect the flow control or data flow of a system. This could allow a remote attacker to gain unauthorized access to sensitive information, create denial of service conditions, or execute arbitrary code.
Affected Configuration(s):

- ExactaMix 1200 versions 1.1, 1.2
- ExactaMix 2400 versions 1.10, 1.11

Affected Products and Versions

The following product configurations are affected:

- ExactaMix 1200 versions 1.1, 1.2, 1.4, 1.5
- ExactaMix 2400 versions 1.10, 1.11, 1.13, 1.14

Mitigations

For those customers that are using ExactaMix EM 2400 versions V1.10, V1.11 and ExactaMix EM1200 versions V1.1, V1.2, Baxter recommends these customers contact their local service support team or regional product service support to upgrade to the ExactaMix v1.4 (EM1200) and ExactaMix v1.13 (EM2400) compounders.

For all customers, Baxter recommends the following compensating controls for all ExactaMix customers including, but not limited to:

- Ensuring appropriate physical controls within its customers environments to protect against unauthorized access to devices.
- Ensuring ExactaMix Compounder passwords are kept as confidential. the customer should implement administrative controls to ensure they are not misused, mismanaged, or other otherwise shared with unauthorized individuals.
- The device should be used only in accordance with its intended use and not for email, Internet access, file sharing or other non-approved use. No software of any kind should be installed on the device unless approved, in writing, by Baxter.
- The ExactaMix Compounder should be segmented from the main customer's 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.

Related Information

If you observe any symptoms that are representative of these vulnerabilities, disable wireless operation of your pump and contact your service representative immediately.

Additional resources:

https://www.us-cert.gov/ics/advisories/icsma-20-170-01

For more information:

For Baxter US technical support contact: 1-800-678-2292

For questions regarding cybersecurity of Spectrum pumps or any Baxter product contact: productsecurity@baxter.com