Baxter Product Security Bulletin

Title: "PrintNightmare" Vulnerability (CVE-2021-34527)
Publication Date: July 23, 2021
Last Update: July 23, 2021

BACKGROUND

This notification applies to customers that utilize Baxter ExactaMix Compounders. The notification provides product security information and recommendations for the Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) which impacts all versions of the Windows Operating System. The vulnerability, commonly referred to as "PrintNightmare", is not exclusive to Baxter or medical devices, and is described in the CERT Coordination Center (CERT/CC) Vulnerability Note (VU#383432).

AFFECTED PRODUCTS

All versions of ExactaMix Compounders contain the Windows Operating System and therefore are impacted by this vulnerability as listed below:

- ExactaMix 1200 v1.1, v1.2 / ExactaMix 2400 v1.10, v1.11
- ExactaMix 1200 v1.4, v1.5 / ExactaMix 2400 v1.13, v1.14

VULNERABILITY DETAILS

"PrintNightmare" is a remote code execution (RCE) vulnerability impacting the Windows Print Spooler service. The vulnerability allows a remote authenticated attacker to execute arbitrary code with SYSTEM privileges on a vulnerable system due to the Microsoft Windows Print Spooler service failing to restrict access to functionality used to allows users to add printers and related drivers. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The vulnerability in the NIST National Vulnerability Database (NVD) has a CVSS 3.1 base score of 8.8 and vector of AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

POTENTIAL IMPACT ON PERFORMANCE, SAFETY, and DATA

The potential impact is dependent on the version of ExactaMix.

1. ExactaMix 1200 v1.1, v1.2 / ExactaMix 2400 v1.10, v1.11

   Baxter has rated the CVSS score as 8.8. If exploited, the "PrintNightmare" vulnerability could result in an authenticated user obtaining elevated privileges via a remote RPC call. This could impact confidentiality and integrity of the system, risk exposure of sensitive information including PHI, and result in delay or interruption of service.

2. ExactaMix 1200 v1.4, v1.5 / ExactaMix 2400 v1.13, v1.14

   Baxter has rated the CVSS score as 6.4. Rationale for this lowered score is reduced exploitability due to implementation of registry key recommendations from Microsoft to enforce permission requests for RPC printer calls, and minimizing loss of confidentiality due to implementation of ExactaMix encrypted database. If exploited, this vulnerability could impact integrity of the system and result in delay or interruption of service.

RESPONSE

As part of our Product Security program, Baxter continues to monitor the available information regarding this reported vulnerability and assess for any potential impact on its products. Baxter will provide an update to this bulletin if necessary.

ExactaMix Cybersecurity Guide recommend customers implement countermeasures to increase the security of ExactaMix, such as placing the product behind the hospital's firewall and isolating it on its own secure VLAN to segregate the system from other hospital systems.

To date, Baxter has not received any reports of this vulnerability impacting clinical use of any Baxter products.

MITIGATIONS & COMPENSATING CONTROLS

The following mitigations reduce the likelihood that "PrintNightmare" will be exploited:

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

For customers not already on the latest version of ExactaMix v1.5 (EM1200) or ExactaMix v1.14 (EM2400), Baxter recommends customers upgrade to these versions.

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

FOR MORE INFORMATION

If you observe any symptoms that are representative of this vulnerability, disconnect your system and contact your service representative immediately.

For Baxter technical support contact:
Baxter US technical support center at 1-800-678-2292, or your local technical support call center

For questions regarding cybersecurity of any Baxter products contact:
productsecurity@baxter.com