Baxter Product Security Bulletin

Multiple Windows SMB Remote Code Execution Vulnerabilities

Publication Date: December 11, 2019
Last Update: December 11, 2019
Version: V1.0

SUMMARY

As part of our Product Security program, Baxter has reviewed the Microsoft security bulletin regarding multiple vulnerabilities in Microsoft Windows, the most severe of which could allow remote code execution if an attacker sends certain messages to a Microsoft Server Message Block 1.0 (SMBv1) server. Unpatched Windows operating systems that rely on SMBv1 contain multiple vulnerabilities that may be exploited by ransomware and other cyber threats (see Microsoft Security Bulletin MS17-010 for the list of vulnerabilities). **Please note that vulnerabilities found on SMBv1 servers are not Baxter-specific vulnerabilities.**

VULNERABILITY DESCRIPTION

We refer customers to the Microsoft website for further information on the Windows SMB Remote Code Execution Vulnerabilities. In short, the remote code execution vulnerabilities could allow a successful attacker to execute code on the target server. Microsoft has made security updates available to resolve these vulnerabilities in Windows.

AFFECTED EXACTAMIX PRODUCTS

The following ExactaMix EM1200 and EM2400 versions run on Windows operating systems that are impacted by the SMBv1 vulnerabilities:

- ExactaMix v1.1/v1.2 (EM1200)
- ExactaMix v1.10/v1.11 (EM2400)

Mitigations

Baxter has launched new versions of the ExactaMix compounder software — ExactaMix v1.4 (EM1200) and ExactaMix v1.13 (EM2400) — which incorporate Microsoft Windows operating system version 10 (Windows 10) and disable SMBv1. Baxter chose to implement the Microsoft recommended workaround of disabling SMBv1 in these new software versions rather than deploying the MS17-010 patch. Please see below for additional compensating controls recommended by Baxter.

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 v1.1/v1.2 (EM1200) and ExactaMix v1.10/v1.11 (EM2400) run on Windows operating systems which have been determined to be susceptible to the SMBv1 vulnerabilities. Baxter recommends all 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 that feature the Microsoft Windows 10 operating system with SMBv1 disabled. 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 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 SMBv1-related resources:

- Microsoft (MS) Customer Guidance for WannaCrypt Attacks
- US-CERT: Indicators Associated with WannaCry Ransomware (TA17-132A)
- ENISA – European Union Agency for Cybersecurity: WannaCry Ransomware Outburst