

## BAXTER EXPANDS CYBERSECURITY COMMITMENT, JOINS FORCES WITH U.S. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) LED PROGRAM

- Baxter joins government sponsored Common Vulnerabilities and Exposures (CVE®) program as a CVE Numbering Authority
- Program identifies, defines and catalogs publicly disclosed cybersecurity vulnerabilities to help enable more rapid identification and resolution

**DEERFIELD, III., FEBRUARY 23, 2022** – Baxter International Inc. (NYSE:BAX), a leading global medtech leader, announced that it has received authorization from the Common Vulnerability and Exposures (CVE®) program to be a CVE Numbering Authority. As a CVE Numbering Authority (CNA), Baxter is responsible for the assignment of CVE identifiers to cyber vulnerabilities for Baxter and Hillrom commercially available products, and for publicly disclosing information about the vulnerabilities in the associated CVE Record. The CVE program is sponsored by the Cybersecurity and Infrastructure Security Agency (CISA), which is part of the U.S. Department of Homeland Security and aims to enable the rapid identification and resolution of cybersecurity issues.

“We remain vigilant in working to protect Baxter devices from cybersecurity threats,” said Talvis Love, senior vice president and chief information officer at Baxter. “Our designation as a CVE Numbering Authority is an extension of these efforts to strengthen cybersecurity across our network and portfolio.”

Cyberattacks against healthcare organizations have risen 45% since Nov. 1, 2020 as compared to a 22% increase in cyberattacks for other industries during the same time period.<sup>1</sup> Cyberattacks are also increasingly growing in sophistication, intensifying the risk to healthcare systems and patients.

A centralized system and process for cataloging cybersecurity vulnerabilities helps stakeholders like device manufacturers, hospital systems and IT teams to more rapidly discover and correlate information used to protect systems against attacks. Technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities. Using standardized and publicly disclosed CVE records can result in significant time and cost savings.



"Our contributions as a CVE Numbering Authority will help support the faster identification, remediation and resolution of potential cybersecurity vulnerabilities and allow hospitals and clinics to continue focusing on providing the highest level of care to patients," said Love.

## About Baxter

Every day, millions of patients, caregivers and healthcare providers rely on Baxter's leading portfolio of diagnostic, critical care, kidney care, nutrition, hospital and surgical products used across patient homes, hospitals, physician offices and other sites of care. For 90 years, we've been operating at the critical intersection where innovations that save and sustain lives meet the healthcare providers who make it happen. With products, digital health solutions and therapies available in more than 100 countries, Baxter's employees worldwide are now building upon the company's rich heritage of medical breakthroughs to advance the next generation of transformative healthcare innovations. To learn more, visit [www.baxter.com](http://www.baxter.com) and follow us on [Twitter](#), [LinkedIn](#) and [Facebook](#).

## About the Common Vulnerabilities Program

The mission of the Common Vulnerabilities and Exposures (CVE®) Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities. The CVE Program is sponsored by the Cybersecurity and Infrastructure Security Agency (CISA), of the U.S. Department of Homeland Security (DHS) and is operated by the MITRE Corporation in close collaboration with international industry, academic, and government stakeholders.

*This release includes forward-looking statements concerning Baxter's authorization as a Common Vulnerabilities and Exposures (CVE) Numbering Authority and anticipated benefits associated with the CVE program. The statements are based on assumptions about many important factors, including the following, which could cause actual results to differ materially from those in the forward-looking statements: demand for and market acceptance for new and existing products; product development risks; product quality or patient safety concerns; breaches or failures of the company's information technology systems or products; satisfaction of regulatory and other requirements; actions of regulatory bodies and other governmental authorities; changes in law and regulations; and other risks identified in Baxter's most recent filing on Form 10-K and other SEC filings, all of which are available on Baxter's website. Baxter does not undertake to update its forward-looking statements.*



**Media Contact**

Colleen Weber, (224) 948-5353  
media@baxter.com

**Investor Contact**

Clare Trachtman, (224) 948-3020  
FOR IMMEDIATE RELEASE

###

---

<sup>1</sup> Check Point: Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again. <https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/> Accessed February 18, 2021.