EINPRESSWIRE

Real-World Harms and Deaths Result from Unsecure Coding Practices

Lack of secure coding is resulting in a wider range of physical world harms, including deaths. Worldwide government agencies are calling for more secure code.

Rebecca Herold, CEO, Privacy & Security Brainiacs

DES MOINES, IA, UNITED STATES, February 13, 2024 /EINPresswire.com/ -- When testifying before the House Select Committee on January 31, 2024, U.S. FBI Director Christopher Wray warned that Chinese hackers are preparing to “wreak havoc and cause real-world harm” to the U.S. Such harms through malicious code have long been possibilities. And such harms through unsecure software code have been exploited many times throughout the past few decades, also resulting in a wide range of harms in the physical world. These are not just from nation-state hacking, which was the focus of Director Wray’s testimony, but harms that resulted from other types of hackers, from malicious insiders (those who work for the organizations where the code is executed), from mistakes, and from software code that had coding errors that were not caught typically because of insufficient testing before real-life use.

Here are just a few examples:

- Software-coding errors, bugs and defects incorrectly showed that money had gone missing at a trusted, centuries-old British government corporation from 1999 through 2015. These computer-code problems were noticed, but nothing was done to fix them. As a result, 700 people working throughout the UK Post Office bank were convicted with some going to prison. This error destroyed livelihoods and reputations. Many victims were bankrupted and lost all of their savings and property. Some committed suicide from the distress it caused. The Post Office had to pay more than £138 million (USD $176 million) in compensation and more lawsuits are proceeding.
- Five patients died after receiving a massive dose of X-rays that were the result of a programming error in a Therac-25 radiation therapy machine. The disaster reportedly was caused by software code errors that made different sections of code try to do the same thing at

the same time.

- An electronic health records system (EHR) made by eClinicalWorks (eCW) used by close to one million healthcare professionals in the U.S. in the late 2000’s was determined to contain “spaghetti code…so buggy that when one glitch got fixed, another would develop.” The results were many and widespread including incorrect patient records, showing the wrong patients’ records to physicians making medical decisions, and “Alarming reports of deaths, serious injuries and near misses — thousands of them — tied to software glitches, user errors or other system flaws have piled up for years in government and private repositories.”
- In 2017, security researchers discovered flawed software in the Medtronic MiniMed and MiniMed Paradigm insulin pumps that could easily be exploited by criminals to administer dangerously low or lethally high insulin levels, both of which could kill the users. The manufacturer had to issue a worldwide recall.

Privacy & Security Brainiacs

- On February 25, 1991, during the Gulf War, a Patriot Missile failure resulted in missing a Scud missile, which struck an American Army barracks, killing 28 soldiers and injuring around 100 other people. This was a result of the computer hardware being used and associated software errors and problems.

> “Secure-coding practices must be adopted by all organizations providing applications used by or impacting the public to reduce the numbers of privacy breaches, security incidents, and physical harms.”
>
> *Rebecca Herold, CEO*

- Software-code errors resulted in a woman being killed by a self-driving car in March, 2018. The number of other smart-car and self-driving car accidents that were ultimately caused by software code errors could fill a book.

- Airbus confirmed that a software configuration error caused an Airbus A400M to crash. The flight-recorder data revealed the software-configuration error. A few months earlier an Ethiopian Boeing 737 Max crash that killed all 157 people on board was subsequently suspected of being caused by the same, or a similar, software error.
- In 2021 multiple reports were published about hackers successfully compromising water-treatment plants in California and Florida and changing software-application settings to poison the water for the communities’ residents.

Poorly coded software can allow for privacy breaches and security incidents but most of the public do not realize that unsecure code can also ruin people's lives and even lead to death. Secure-coding practices can significantly help to ensure such tragedies do not occur. Government agencies throughout the world are sounding the alarm, telling tech companies to practice secure coding to improve public safety.

Dr. M.E. Kabay

Cybersecurity expert, educator, and NSA-accredited university-program creator, Dr. M. E. Kabay, is creating and delivering courses for the online education platform Privacy & Security Brainiacs (PSB), and explains how the concepts he teaches in his Secure Coding course can provide the information programmers and information-technology managers need to avoid creating harmful and deadly software. In the introduction to his course, Dr Kabay writes,

- The issues include not only technical issues such as avoiding specific types of problems but also having to manage people so they can focus on something they usually don't like: showing that there are mistakes in the code. Showing that there are no errors can consist merely of failing to test thoroughly.
- There are administrative issues, too, such as avoiding conflicts of interest. For instance, the director of software quality assurance must NOT report to the director of programming; they should both report as equals to the Chief Information Officer of the organization.
- Technical issues include:

o Thorough documentation of the code by the designers and programmers;
o Using local variables, not global variables, when storing sensitive data;
o Reinitializing temporary storage immediately after the last legitimate use;
o Limiting functionality of each module to the specific requirements;
o Limiting access to sensitive data in databases;
o Using strong, well-established encryption;
o Never allowing access by programmers to production data (only copies);
o Masking sensitive data when generating test-data sets;
o Using test-coverage monitors;
o Integrating detailed logging into all applications;
o Using record-level locking;
o Applying digital signature techniques for authenticating code and preventing hacks.

Dr. Kabay provides detailed descriptions and examples about these in his Secure Coding course includes a 20-question online exam generated at random from a list of over 60 questions available for study by the students, certificate for passing the course exam that contains information to support continuing professional education (CPE) requirements for a wide range of certifications, and access to communicate directly with Dr. Kabay through the PSB course-messaging portal to ask him questions related to the course topics and to engage in professional discussions.

“The impacts of not using secure code throughout our society are widespread, harmful, and deadly. And they are getting worse. As one example, consider that artificial intelligence (AI) tools are being adopted at unprecedented speed. AI, very simply put, is accomplished through the use of software-coded algorithms. Virtually all AI tools are being used without demonstrated objective, explicitly verified confirmation that accurate security and privacy practices have been engineered within that code and thoroughly tested. Secure-coding practices would help to provide such verification, when performed by impartial entities,” explained Ms. Herold. “Secure-coding practices must be adopted by all organizations that provide applications used by, or impacting, the general public to reduce the growing numbers of privacy breaches, security incidents, and physical harms. Dr. Kabay’s Secure Coding course can help organizations to meet this secure coding goal.”

About Privacy & Security Brainiacs
Ms. Herold launched Privacy Security Brainiacs in partnership with her son Noah Herold. The online platform offers IT, security, privacy and compliance education, training and awareness tools to help organizations of all sizes and in a wide range of industries throughout the world. Privacy & Security Brainiacs provides online Software as a Service (SaaS) education services, with business admin capabilities for organizations to assign and manage training and other educational activities for their employees. They also provide policies and procedures templates, forms, videos, podcasts, e-books, paperback books, custom training, awareness events, supplemental materials and learning activities. To learn more, visit privacysecuritybrainiacs.com.

# # #

Media Contacts:

Rebecca Herold (for Privacy & Security Brainiacs), rebeccaherold@privacysecuritybrainiacs.com
Noah Herold (for Privacy & Security Brainiacs), noahherold@privacysecuritybrainiacs.com

ADDITIONAL INFORMATION:
PSB offers a sliding scale to lower prices as the number of learner attendees increases, as well as a price break of 50% off for clients agreeing to become beta testers of new courses as they are developed. Organizations interested in these arrangements are encouraged to contact PSB at info@privacysecuritybrainiacs.com.

The PSB online courses service offers a variety of benefits for individual IT professionals, as well as for business leaders in charge of their organizations’ training strategies. The initial purchase of a course establishes a free administrator account that can manage additional learners whom the administrator manages. The PSB platform provides an extensive administrator and learner tracking-and-reporting portal and access to a wide range of functionality.

From the portal, administrators can track the training activities of learners, view quiz results, push classes and supplemental materials to learners and create certificates for learners who have completed their assigned course. Special certificates are available for those who pass quizzes, as well as those who pass with exceptional scores. Private learning portals for each learner display the learner's course history, including details like course title, completion date and time, quiz results, access to past courses and materials, as well as communication options for the learner and the administrator.

Rebecca Herold
Privacy and Security Brainiacs
+ +1 515-491-1564
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube