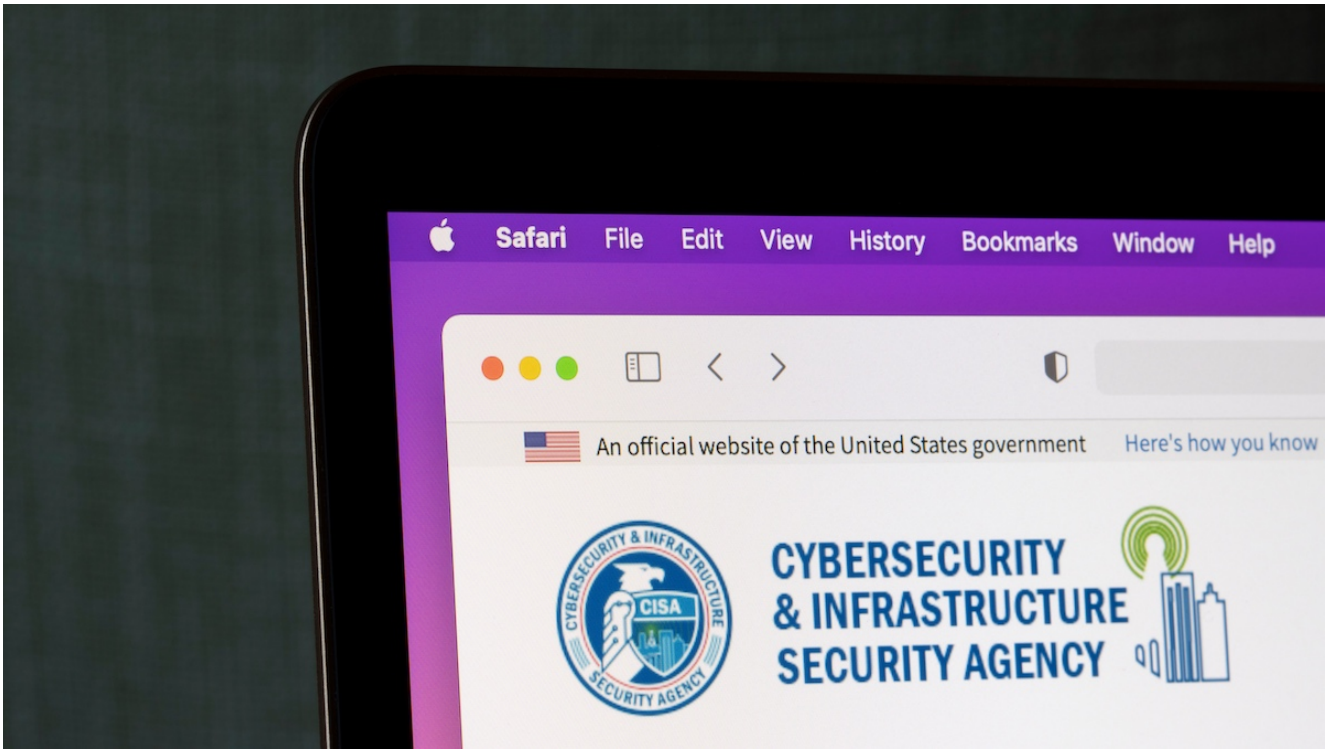
CISA Introduces Secure-by-design and Secure-by-default Development Principles



CISA has described and published a set of principles for the development of security-by-design and security-by-default cybersecurity products.

Pillar Three of the National Cybersecurity Strategy published on March 1, 2023 is titled 'Shape market forces to drive security and resilience'. Within this section the Administration makes two points very clear. Firstly, security liability must be shifted away from the use of security products to the development of security products; and secondly, federal procurement power will be used to encourage this shift.

Both points were previewed in a speech given by CISA director Jen Easterly at Carnegie Mellon days earlier (February 27, 2023). She noted that insecurity has become normalized, and that the onus is currently on the user to make use of products

less risky. She said this must change, so that the user is forced into making usage more rather than less risky.

This requires products to be built with security-by-design and security-by-default principles – and she noted that government has two incentives to ensure this: regulations, and federal procurement power.

Now, on April 13, 2023, CISA published a set of principles (PDF) that developers can employ to achieve these ends. The principles were developed with collaboration between CISA, the NSA and the FBI, and foreign security agencies including those from Australia, Canada, and the UK.

The security-by-design principles acknowledge that they will not prevent all breaches and will likely increase development costs; but also note that they will improve the nation's cybersecurity and reduce the developers' ongoing maintenance and patching costs.

Top of the list of design principles is the use of memory safe programming languages. In her earlier speech, Easterly had commented that around two-thirds of known vulnerabilities are 'memory safety' vulnerabilities. "Certain programming languages," she said, "most notably, C and C++, lack the mechanisms to prevent coders from introducing these vulnerabilities into their software. By switching to memory safe programming languages—like Rust, Go, Python, and Java—these vulnerabilities can be eliminated." The principles add C# and Swift to the memory safe list.

Other principles include the use of a secure hardware foundation, secure software components, parameterized queries to avoid SQL injection attacks, and SAST and DAST testing. These should be supported by code reviews, SBOMs, vulnerability disclosure programs and more.

Security-by-default refers to the practice of delivering products that are secure out-of-the-box, rather than products

that must be made secure by the user. The principle notes that ‘hardening guides’ (which can be used by attackers as a roadmap by attackers) should be reversed into ‘loosening guides’ that explain which changes users should make while also listing the resulting security risks.

This can be achieved by following the security-by-default principles, which include elements such as no default password, mandated MFA, single sign on via modern open standards, and secure logging. “The authoring agencies believe that developing written roadmaps and executive support that prioritize these ideas into an organization’s most critical products is the first step to shifting towards secure software development practices,” notes CISA.

But it’s not solely down to the developer to willingly adopt these principles. Customers are encouraged to insist on buying demonstrably secure-by-design and secure-by-default products. “IT departments should be empowered to develop purchasing criteria that emphasize the importance of Secure-by-Design and Secure-by-Default practices (both those outlined in this document and others developed by the organization),” says CISA. “Furthermore, IT departments should be supported by executive management when enforcing these criteria in purchasing decisions.”

The purpose in developing this set of principles is nothing less than an attempt to improve the cybersecurity of the entire nation in the face of increasing criminal and increasingly dangerous adversarial nation threats. Easterly mentioned two possible incentives: regulation and federal purchasing power. The Administration has already made clear that it will use its purchasing power to help persuade developers to comply.

It follows that there are two important reasons for developers to understand and use the CISA principles. Firstly, it is the right thing to do. Secondly, if there is to be any hope of

selling into the federal government, it is the essential thing to do.

Related: White House Cybersecurity Strategy Stresses Software Safety

Related: NSA Publishes Guidance on Mitigating Software Memory Safety Issues

Related: Companies Announced Billions in US Government Cybersecurity Contracts in 2022

Related: AWS Enables Default Server-Side Encryption for S3 Objects

> *CISA Introduces Secure-by-design and Secure-by-default Development Principles*