Secure by Design Alert: Eliminating Cross-Site Scripting Vulnerabilities

Malicious Cyber Actors Use Cross-Site Scripting Vulnerability to Compromise Systems

CISA and FBI are releasing this Secure by Design Alert as a part of our ongoing effort to reduce the prevalence of vulnerability classes at scale. Vulnerabilities like cross-site scripting (XSS) continue to appear in software, enabling threat actors to exploit them. However, cross-site scripting vulnerabilities are preventable and should not be present in software products.

Senior executives and business leaders should ask their teams how they are working to eliminate these defects and whether they are implementing a secure by design approach in their products.

> Despite having had extensive knowledge and effective solutions for cross-site scripting vulnerabilities for over twenty years, many software manufacturers continue to release products with these flaws, thereby exposing customers to unnecessary risks.

Cross-site scripting vulnerabilities arise when manufacturers fail to properly validate, sanitize, or escape inputs. These failures allow threat actors to inject malicious scripts into web applications, exploiting them to manipulate, steal, or misuse data across different contexts. Although some developers employ input sanitization techniques to prevent XSS vulnerabilities, this approach is not infallible and should be reinforced with additional security measures.

CISA and FBI urge **CEOs and other business leaders** at technology manufacturers to direct their technical leaders/teams to review past instances of these defects and create a strategic plan to prevent them in the future.

To further prevent these vulnerabilities, **technical leaders** should:

- Review their written threat models,
- Ensure software validates input for both structure and meaning,[1]
- Use modern web frameworks that offer easy-to-use functions for output encoding to ensure proper escaping or quoting,[2]
    - By distinguishing user input from application code, these frameworks make it so that the burden doesn't fall on developers to correctly escape user input every time. Follow the framework's guidance for preventing any remaining edge cases that may lead to XSS vulnerabilities.
    - When unable to use modern web frameworks, ensure that all user input displayed in web applications undergoes proper escaping or sanitization.
- Conduct code reviews,
- And implement aggressive adversarial product testing to ensure the quality and security of their code throughout the development lifecycle.[3]

[1] Input Validation Cheat Sheet. OWASP Cheat Sheet Series. https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
[2] "Cross-Site Scripting Prevention Cheat Sheet." OWASP Cheat Sheet Series. https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
[3] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). Secure Software Development Framework | CSRC | CSRC. https://csrc.nist.gov/Projects/ssdf

Secure By Design Lessons to Learn

Products that are secure by design reasonably protect against malicious cyber actors exploiting the most common and dangerous classes of product defects. Incorporating security at the outset—beginning in the design phase and continuing throughout development, release, and updates—reduces the burden on customers and risk to the public. The cybersecurity community has considered easily exploitable authentication vulnerabilities to be "unforgivable" since 2007.

Despite this finding, cross-site scripting vulnerabilities—many of which are the result of CWE-79—remain a prevalent class of defect.[4]

Secure By Design Principles to Follow

CISA and FBI encourage manufacturers to learn how to protect their products from falling victim to cross-site scripting exploits and other preventable malicious activity by reviewing the three principles laid out in the joint guidance Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.

Principle 1: Take Ownership of Customer Security Outcomes

Software manufacturers must prioritize customer security by eliminating cross-site scripting vulnerabilities from their products. Key security investments should include providing secure building blocks for developers to prevent single errors from compromising millions of users' data. Relying solely on detecting, mitigating, and patching vulnerabilities after they have been identified for years is not a sustainable security approach. Instead, manufacturers should implement effective mechanisms to prevent vulnerabilities on a large scale early in the development cycle.

Adopting standard best practices, such as those mentioned above, can help manufacturers root out cross-site scripting vulnerabilities at the source, as opposed to depending on customers to apply fixes. Automated safeguards should be implemented to prevent software from utilizing unsafe functions, complemented by the use of static analysis tools to identify improper handling of user input. These measures, combined with rigorous code reviews, can detect flaws before software deployment.

Additionally, senior executives at software manufacturers must take accountability for customer security starting by regularly testing and conducting code reviews to assess product susceptibility to exploitation. Guidance from organizations like the Open Web Application Security Project (OWASP) and others offers proven methods and techniques for conducting thorough testing.

Principle 2: Embrace Radical Transparency and Accountability

Manufacturers should lead with transparency when disclosing product vulnerabilities. To that end, manufacturers should track the vulnerability associated with their products and disclose these to their customers via the CVE program. Manufacturers should ensure that their CVE records are complete, accurate, and timely. In addition to providing CVEs, it is especially important that manufacturers supply an accurate CWE so the industry can track classes of software defect, and customers can understand areas where a given vendor's development practices may require improvement.[5]

Many, but not all, cross-site scripting vulnerabilities are the result of CWE-79. As such, manufacturers should identify and document the root causes of cross-site scripting vulnerabilities and declare it a business goal to work toward eliminating the entire class. Software manufacturers should also maintain a modern vulnerability disclosure program (VDP). **Note:** CISA provides resources to assist organizations in establishing and maintaining a VDP.

---

[4] "2023 CWE Top 25 Most Dangerous Software Weaknesses." MITRE's CWE Top 25, 2023. https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

[5] Common Weakness Enumeration (CWE) classification identifies classes of software/hardware weaknesses (including vulnerabilities and defects); Common Vulnerabilities and Exposures (CVE) classification identifies and labels unique vulnerabilities in specific software/hardware products.

Principle 3: Build Organizational Structure and Leadership to Achieve These Goals

Technology manufacturing executives should:

- Give the security of their products the same level of care they give to cost.
- Consider the full picture: that customers, our economy, and our national security are currently bearing the brunt of business decisions to not build security into their products.
- Be aware that fully implementing secure by design software development can reduce financial and productivity costs as well as complexity.
- Make the appropriate investments and develop the right incentive structures that promote security as a stated business goal.
- Lead programs to root out entire classes of vulnerability rather than addressing them on a case-by-case basis.
- Establish organizational structures that prioritize proactive measures, such as adopting standard best practices, to root out cross-site scripting vulnerabilities at the source.
- Ensure their organization conducts reviews to detect common and well-known vulnerabilities, like cross-site scripting, to determine their susceptibility, and implement the existing effective and documented mitigations.
    - Organizations should conduct these reviews continually to root out classes of vulnerability, as some classes of defect may change or develop over time.
    - Executives should request regular updates to assess: (1) the company's progress at identifying recurring classes of vulnerability, (2) the company's progress to eliminate them, and (3) the appropriate resources needed to continue making progress.

Action Item For Software Manufacturers

To demonstrate their commitment to building their products that are secure by design, software manufacturers should consider taking the Secure by Design Pledge. The pledge lays out seven key goals that the signers commit to demonstrating measurable progress towards, including reducing systemic classes of vulnerability like cross-site scripting.

This Secure by Design Alert is part of an ongoing series that aims to advance industry-wide best practices that eliminate entire classes of vulnerability during the design and development phases of the product development lifecycle. Through the Secure by Design initiative, we seek to foster a cultural shift across the industry by normalizing the development of technology products that are secure to use out of the box. Visit cisa.gov to learn more about the principles of Secure by Design, take the Secure by Design Pledge, and stay informed on the latest Secure by Design Alerts.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.