DATE: 03-29-2025
TO: Bridget Bean, CISA
FROM: Charles Moye
SUBJECT: Mitigating JavaScript Injection Attacks on Websites

JavaScript injection attacks remain a persistent threat to website security. Time and time again, they have been used to compromise sensitive data, disrupt services, and enable malicious actors to gain unauthorized access to systems. These attacks exploit vulnerabilities in input validation and script execution, which can allow attackers to manipulate web apps and execute arbitrary code in a user's browser.

These attacks are frequent and can be utilized in large scales. Recently, this form of attack was used to display an overlay promoting Chinese gambling websites on upwards of 100,000 sites, as per HackerNews. Incidents such as this highlight the legitimacy of the vulnerability, and the importance of dedicating more resources to curb its scope. These breaches may affect both government and private websites, and can expose users to risks such as data theft, credential compromise, and malware. This issue is of significant importance due to the widespread adoption of JS in web development.

To address this issue, CISA must consider taking measures to mitigate it. Frequent updates to best practices for secure JS implementation is a no-brainer and good first step. Offering a training program on JS security would likely be appreciated by web developers, as this issue can be the result of both a front end developer or a back end developer. More effective would be a certification of similar credibility to CompTIA, as it would provide hands-on training for what steps must be taken when implementing JS securely, and would also allow companies to seek employees who have earned this certification.

By implementing these measures, CISA can make the internet a safer place by allowing users to have peace of mind while they browse and by allowing developers to be more confident in the security of their code. Strengthening defenses against this threat is crucial for maintaining integrity and trust on online platforms.

https://thehackernews.com/2025/03/150000-sites-compromised-by-javascript.html