Web Application Attacks Intensify in Fourth Quarter of 2023, According to New Edgio Quarterly Attack Trends Report

February 22, 2024

Leading edge platform provider identifies new attack patterns and ways for organizations to best protect digital assets, in inaugural issue of quarterly threat report

PHOENIX--(BUSINESS WIRE)--Feb. 22, 2024-- Edgio (NASDAQ: EGIO), the platform of choice for speed, security, and simplicity at the edge, found that web application attacks continued to increase and evolve in the fourth quarter of 2023, as reported in its new Edgio Quarterly Attack Trends Report in which the company analyzed 5.2 billion attack requests. Edgio found that the most prevalent attack mitigated was path traversal. A successful path traversal attack allows a threat actor to access files on a web server, and has surpassed the prior #1 threat, SQL injection, a common attack vector that often uses malicious SQL statements to attempt to exfiltrate sensitive data from databases behind applications.

Edgio's report explains how path traversal attacks can lead to deep system intrusions posing a significant threat to an organization's infrastructure and the confidentiality, integrity, and availability of data delivered over the Internet. These attacks can result in unauthorized access to content, the loss of personally identifiable information (PII), the dissemination of private/copyrighted information, or even remote code execution. Unmitigated attacks can lead to even more serious consequences, such as the deployment of ransomware or other malicious software.

"As one of the leading edge-computing providers, Edgio has unparalleled visibility into the threats facing web applications today," said Tom Gorup, Vice President of Security for Edgio. "We are assembling our knowledge and expertise into a quarterly read-out to enable enterprises to better protect their web infrastructure and applications. As more businesses become dependent on their digital assets, it's critical this knowledge is shared to build a safer Internet."

The report looked at malicious requests and the different types of blocking, categorizing protection into three categories: access control rules, managed rulesets, and custom signatures. Of those that were focused on access controls, over 76% of mitigated requests were based on IP, user-agent, and country matches, highlighting just how much bad traffic can be eliminated with basic blocklisting tactics. With managed rulesets, Edgio saw a wide range of threat types blocked, with path traversal, SQL injection and cross-site scripting (XSS) attacks leading the way when it comes to OWASP attacks.

In addition, Edgio was able to review web application firewall (WAF) request denials by country of origin, while noting that attackers often leverage local resources to launch attacks in order to evade geofencing tactics. This could explain why attacks coordinated from advanced threat actors in more prominent countries did not crack Edgio's Top 10 for the quarter.

Top countries by malicious request origin, making up nearly 62% of all requests denied, include:

- United States – 26.3%
- France – 17.4%
- Germany – 9.4%
- Russia – 8.8%

Edgio found that WAF customers used access control features to allow or deny specific request methods, using their knowledge of their own applications to inform their security controls and lower risk. The report indicates that attackers frequently leverage request methods like HEAD that return app and infrastructure information that can be used by the attacker for reconnaissance purposes and to craft a malicious payload.

Based on deep parsing of attack payloads, Edgio found that 98% of all malicious payloads fell into JavaScript Object Notation (JSON) and URL encoded form categories (used for storing and transporting data) but cautioned security teams to remain vigilant as attackers evolve in their selection of payload content types.

Best practices for digital asset protection: proactively stop threats against websites and applications

Based on its findings, Edgio recommends the following methods to best protect digital assets, including websites and applications:

- Ensure your WAF provides a layered defense to protect organizations against the known bad, application-specific, and emerging threats. A complete solution will show a distribution of enforcement across access control rules, managed rulesets, and custom signatures.
- Blocklists are still an effective and low-cost part of a layered security approach to safeguard Internet-facing assets. Organizations should also take advantage of threat intelligence feeds to further harden their security posture against known bad actors.
- While managed rules are often maintained and updated by your WAF provider, it is not advisable to use a 'set it and forget' approach. As an application evolves and new functionalities are developed, policy reviews and analysis of managed ruleset enforcement is recommended. It is best to ensure rules are closely aligned with business application needs.
- Organizations should take the time to understand where they are doing business and where they aren't allowed to do business. Block the countries or sub-regions that bring no value to a brand to reduce their attack surface. Blocking embargoed countries is a great starting point, but don't rely on this approach as a catch all for bad actors.

- Know the application and use this knowledge to inform security solutions, like a WAF, to limit the application request methods or content types based on application needs.

To obtain a full copy of the report, click here.

About Edgio

Edgio (NASDAQCM: EGIO) helps companies deliver online experiences and content faster, safer and with more control. Our developer-friendly, globally scaled edge network, combined with our fully integrated application and media solutions, provides a single platform for delivering high-performing, secure web properties and streaming content. Companies can deliver content quicker and more securely through this fully integrated platform and end-to-end edge services, boosting overall revenue and business value. To learn more, visit edg.io and follow us on Twitter, LinkedIn and Facebook.

View source version on businesswire.com: https://www.businesswire.com/news/home/20240222674952/en/

Media:
Sally Winship Comollo
swinship-comollo@edg.io

Source: Edgio