CSP: script-src unsafe-inline

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Medium	1 target	0 days ago

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

Instances (1 of 6)

uri: https://safeuseledcstg.wpenginepowered.com/
method: GET
param: Content-Security-Policy
evidence: default-src safeuseledcstg.wpenginepowered.com 'self' data: 'unsafe-inline' 'unsafe-hashes' 'unsafe-eval'
otherinfo: script-src includes unsafe-inline.

References

https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
https://github.com/HtmlUnit/htmlunit-csp
https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Vulnerable Target	First Detected	Last Detected
https://safeuseledcstg.wpenginepowered.com/ Staging	0 days ago	0 days ago