Semgrep SAST Scan Report for Repository: Semgrep-Demo/ Cesar-JsGithubAPI

Report Generated at 2024-09-04 21:52

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	0
Findings- SAST Medium Severity	4
Findings- SAST Low Severity	1

Findings Summary- High Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location

Findings Summary- Medium Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
path-join-resolve-traversal	Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.	medium	open	main	githubWorkflow.js#L78
path-join-resolve-traversal	Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.	medium	open	main	githubWorkflow.js#L103
path-join-resolve-traversal	Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.	medium	open	main	githubWorkflow.js#L120
path-join-resolve-traversal	Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.	medium	open	main	githubWorkflow.js#L162

Findings Summary- Low Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
unsafe-formatstring	Detected string concatenation with a non-literal variable in a util.format / console.log function. If an attacker injects a format specifier in the string, it will forge the log message. Try to use constant values for the format string.	low	open	main	githubWorkflow.js#L187