# CVE Detail – CVE-2020-25095

LogRhythm Platform Manager (PM) 7.4.9 allows CSRF. The Web interface is vulnerable to Cross-site WebSocket Hijacking (CSWH). If a logged-in PM user visits a malicious site in the same browser session, that site can perform a CSRF attack to create a WebSocket from the victim client to the vulnerable PM server. Once the socket is created, the malicious site can interact with the vulnerable web server in the context of the logged-in user. This can include WebSocket payloads that result in command execution.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.36583

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-352: Cross-Site Request Forgery (CSRF)

## CAPEC(s)

* CAPEC-111: JSON Hijacking (aka JavaScript Hijacking)
* CAPEC-462: Cross-Domain Search Timing
* CAPEC-467: Cross Site Identification
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:a:logrhythm:platform\_manager:7.4.9:\*:\*:\*:\*:\*:\*:\*