# CVE Detail – CVE-2018-6651

In the uncurl\_ws\_accept function in uncurl.c in uncurl before 0.07, as used in Parsec before 140-3, insufficient Origin header validation (accepting an arbitrary substring match) for WebSocket API requests allows remote attackers to bypass intended access restrictions. In Parsec, this means full control over the victim's computer.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.44804

## CVSS Scoring

CVSS v3.0 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:uncurl\_project:uncurl:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:parsecgaming:parsec:\*:\*:\*:\*:\*:\*:\*:\*