# CVE Detail – CVE-2020-9437

SecureAuth.aspx in SecureAuth IdP 9.3.0 suffers from a client-side template injection that allows for script execution, in the same manner as XSS.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.69387

## CVSS Scoring

CVSS v3.1 Score: 4.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## CAPEC(s)

* CAPEC-209: XSS Using MIME Type Mismatch
* CAPEC-588: DOM-Based XSS
* CAPEC-591: Reflected XSS
* CAPEC-592: Stored XSS
* CAPEC-63: Cross-Site Scripting (XSS)
* CAPEC-85: AJAX Footprinting

## Affected Products

* cpe:2.3:a:secureauth:secureauth\_identity\_provider:9.3.0:-:\*:\*:\*:\*:\*:\*