Sony BRAVIA Digital Signage 1.7.8 Insecure Direct Object Reference

2020.12.04

Credit: **LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)**

Risk: **Low**

Local: **No**

Remote: **No**

CVE: **N/A**

CWE: **N/A**

Sony BRAVIA Digital Signage 1.7.8 Client-Side Protection Bypass / IDOR

Vendor: Sony Electronics Inc.
Product web page: https://pro-bravia.sony.net
https://pro-bravia.sony.net/resources/software/bravia-signage/
https://pro.sony/ue_US/products/display-software
Affected version: <=1.7.8

Summary: Sony's BRAVIA Signage is an application to deliver video and still images to Pro BRAVIAs and manage the information via a network. Features include management of displays, power schedule management, content playlists, scheduled delivery management, content interrupt, and more. This cost-effective digital signage management solution is ideal for presenting attractive, informative visual content in retail spaces and hotel reception areas, visitor attractions, educational and corporate environments.

Desc: Insecure direct object references occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorizati

```
on
and access the hidden '/#/content-creation' resource in the syste
m.

Tested on: Microsoft Windows Server 2012 R2
           Ubuntu
           NodeJS
           Express


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2020-5611
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-20
20-5611.php


20.09.2020

--


http://192.168.1.20:8080/#/content-creation
```

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)