Cayin Content Management Server 11.0 Root Remote Command Injection

Title: Cayin Content Management Server 11.0 Root Remote Command Injection
Advisory ID: ZSL-2020-5570
Type: Local/Remote
Impact: System Access, DoS
Risk: (4/5)
Release Date: 04.06.2020

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.

Description

CAYIN CMS suffers from an authenticated OS semi-blind 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 POST parameter in system.cgi page.

Vendor

CAYIN Technology Co., Ltd. - https://www.cayintech.com

Affected Version

CMS-SE v11.0 Build 19179
CMS-SE v11.0 Build 19025
CMS-SE v11.0 Build 18325
CMS Station (CMS-SE-LXC)
CMS-60 v11.0 Build 19025
CMS-40 v9.0 Build 14197
CMS-40 v9.0 Build 14099
CMS-40 v9.0 Build 14093
CMS-20 v9.0 Build 14197
CMS-20 v9.0 Build 14092
CMS v8.2 Build 12199
CMS v8.0 Build 11175
CMS v7.5 Build 11175

Tested On

Apache/1.3.42 (Unix)

Vendor Status

[15.05.2020] Vulnerability discovered.
[23.05.2020] Vendor contacted.
[25.05.2020] Vendor responds asking more details.
[25.05.2020] Sent details to the vendor.
[04.06.2020] No response from the vendor.
[04.06.2020] Public security advisory released.

PoC

cayin_cms.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://www.exploit-db.com/exploits/48553
[2] https://packetstormsecurity.com/files/157944
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/182925
[4] https://cxsecurity.com/issue/WLB-2020060076
[5] https://blog.rapid7.com/2020/06/19/metasploit-wrap-up-69/
[6] https://github.com/rapid7/metasploit-framework/pull/13607
[7] https://www.rapid7.com/db/modules/exploit/linux/http/cayin_cms_ntp
[8] https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/http/cayin_cms_ntp.rb
[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7357
[10] https://packetstormsecurity.com/files/158139

Changelog

[04.06.2020] - Initial release
[05.06.2020] - Added reference [1], [2] and [3]
[22.06.2020] - Added reference [4], [5], [6], [7], [8] and [9]
[03.07.2020] - Added reference [10]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Rete mirabilia**
- **We Suggest**
- **Profiles**
- Site Meter