Cayin Digital Signage System xPost 2.5 Pre-Auth SQLi Remote Code Execution

Title: Cayin Digital Signage System xPost 2.5 Pre-Auth SQLi Remote Code Execution
Advisory ID: ZSL-2020-5571
Type: Local/Remote
Impact: System Access, DoS
Risk: (5/5)
Release Date: 04.06.2020

Summary

CAYIN xPost is the web-based application software, which offers a combination of essential tools to create rich contents for digital signage in different vertical markets. It provides an easy-to-use platform for instant data entry and further extends the usage of CAYIN SMP players to meet users' requirements of frequent, daily maintenance.

Description

CAYIN xPost suffers from an unauthenticated SQL Injection vulnerability. Input passed via the GET parameter 'wayfinder_seqid' in wayfinder_meeting_input.jsp is not properly sanitised before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code and execute SYSTEM commands.

Vendor

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

Affected Version

2.5.18103
2.0
1.0

Tested On

Microsoft Windows 10 Home
Microsoft Windows 8.1
Microsoft Windows Server 2016
Microsoft Windows Server 2012
Microsoft Windows 7 Ultimate SP1
Apache Tomcat/9.0.1
MySQL/5.0

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_xpost.py

Credits

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

References

[1] https://www.exploit-db.com/exploits/48558
[2] https://packetstormsecurity.com/files/157946
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/182922
[4] https://exchange.xforce.ibmcloud.com/vulnerabilities/182923
[5] https://cxsecurity.com/issue/WLB-2020060079
[6] https://blog.rapid7.com/2020/06/19/metasploit-wrap-up-69/
[7] https://github.com/rapid7/metasploit-framework/pull/13607
[8] https://www.rapid7.com/db/modules/exploit/windows/http/cayin_xpost_sql_rce
[9] https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/http/cayin_xpost_sql_rce.rb
[10] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7356
[11] https://packetstormsecurity.com/files/158141

Changelog

[04.06.2020] - Initial release
[05.06.2020] - Added reference [1], [2], [3] and [4]
[22.06.2020] - Added reference [5], [6], [7], [8], [9] and [10]
[03.07.2020] - Added reference [11]

Contact

Zero Science Lab

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

- **Rete mirabilia**

- ## We Suggest

- ## Profiles

- Site Meter