Penetration Test Report
Retest

Prepared for：
HIWIN TECHNOLOGIES CORPORATION

Version-V1.0
October 7th, 2024
Issued by Acer E-Enabling Service Business Inc.

【Table of Contents】

Executive Summary 1

1. List of Severity and Quantity for Tested Targets 2
2. List of Vulnerabilities by Risk for Tested Targets 3
3. Penetration Testing Execution Results 4

Project Plan 6

1. Execution Period and Duration 6
2. Execution Details 6
3. Execution Scope 9

Penetration Testing Execution Results 10

1. SCM 10
2. GlobalProtect Portal 20
3. HIWIN Technologies Corp. Official Website 24
4. HCRM 43
5. Mail 49

Conclusion 54

1. Logic Vulnerability 54
2. Session Management 54
3. Setting Management 54
4. User Authentication 54
5. Email Service Package 54

【List of Tables】

Table 1 Description of Severity 1
Table 2 Target List 2
Table 3 Table of Severity and Quantity 2
Table 4 List of Severity and Quantities for Each Target 2
Table 5 Vulnerability of Tested Targets 3
Table 6 Execution Items and Results for this Project 4
Table 7 Execution Items of Penetration Testing Service 7
Table 8 The Target List of Penetration Test 9
Table 9 SCM-weak cipher suite supported(Medium) 13
Table 10 SCM- Error message is too detailed(Medium) 15
Table 11 SCM- Unrestricted Upload of File (Medium) 17
Table 12 GlobalProtect Portal- weak cipher suite supported (Medium) 22
Table 13 HIWIN Technologies Corp. Official Website-Support for deprecated SSL/TLS protocols(Medium) 28
Table 14 HIWIN Technologies Corp. Official Website-weak cipher suite supported (Medium) 29
Table 15 HIWIN Technologies Corp. Official Website-Enumerable user account (Medium) 32
Table 16 HIWIN Technologies Corp. Official Website-Session fixation (Medium) 34
Table 17 HIWIN Technologies Corp. Official Website-Captcha reuse (Medium) 36
Table 18 HIWIN Technologies Corp. Official Website- Error message is too detailed (Medium) 39
Table 19 HIWIN Technologies Corp. Official Website-Session Cookie has no Secure attribute set (Low) 41
Table 20 HCRM-weak cipher suite supported(Medium) 46
Table 21 Mail-No SMTP Authentication (Medium) 50

Executive Summary

Our company assesses the severity of all testing targets based on the CVSS 3.1(Common Vulnerability Scoring System) scoring standard.

The following table outlines the general rules for assigning severity to identified vulnerabilities:

Table 1 Description of Severity

Severity	CVSS Score	Definition
Critical	9.0-10.0	The tested target can be easily exploited to give attackers possibilities of gaining administrative access, service interruption, or confidential information leakage. Risks must be urgently dealt with and patched based on cybersecurity considerations.
High	7.0-8.9	The tested target has the possibility of intrusion to gain administrative access, service interruption, or confidential information leakage. Risks need to be patched and addressed within a certain deadline due to cybersecurity considerations.
Medium	4.0-6.9	The tested target may be indirectly exploited to give attackers possibilities of gaining administrative access, service interruption, or confidential information leakage. Risks can be patched and addressed depending on the situation within a certain deadline due to cybersecurity considerations.
Low	0.1-3.9	The target of the test has the potential for indirect utilization in intrusion. However, in the current space-time environment, attacks cannot be implemented yet. Providing additional system or network information to attackers poses a potential threat. They are unable to destroy information or cause any system interruptions. In the future, depending on different circumstances, this threat may escalate to a medium to high-severity. From a cybersecurity perspective, it is advisable to assess and prioritize the risks involved and make appropriate improvements based on the situation.
None(Info)	0.0	

1. List of Severity and Quantity for Tested Targets

In sequence of the tested targets, the following table lists all included severity along with their respective quantity of vulnerabilities.

(1) Target List

Table 2 Target List

NO.	Target	Target Name
1.	https://scm.hiwin.tw/	SCM
2.	https://vpn.hiwin.tw/	GlobalProtect Portal
3.	https://www.hiwin.tw/	HIWIN Technologies Corp. Official Website
4.	https://hcrm.hiwin.tw/crm	HCRM
5.	mail.hiwin.tw	Mail

(2) Table of severity and quantity of Tested Targets

The summary of the penetration First Test (FT) and Retest (RT) results is presented in the following table.

Table 3 Table of Severity and Quantity

Severity	Quantity (FT/RT)
Critical	0
High	0
Medium	12/2
Low	1/0
Info	0

The quantity of vulnerabilities for each severity are tabulated according to different targets.

Table 4 List of Severity and Quantities for Each Target

Target	Severity	Quantity (FT/RT)
https://scm.hiwin.tw/ SCM	Critical	0
	High	0
	Medium	3/1
	Low	0
	Info	0
https://vpn.hiwin.tw/ GlobalProtect Portal	Critical	0
	High	0
	Medium	1/0
	Low	0

Target	Severity	Quantity (FT/RT)
	Info	0
https://www.hiwin.tw/ HIWIN Technologies Corp. Official Website	Critical	0
	High	0
	Medium	6/1
	Low	1/0
	Info	0
https://hcrm.hiwin.tw/crm HCRM	Critical	0
	High	0
	Medium	1/0
	Low	0
	Info	0
mail.hiwin.tw Mail	Critical	0
	High	0
	Medium	1/0
	Low	0
	Info	0

2. List of Vulnerabilities by Risk for Tested Targets

In order of tested targets, all vulnerabilities are listed, including the names, Quantity, severity, and potential risks they may cause.

Table 5 Vulnerability of Tested Targets

Target	Severity	Number (FT/RT)	Vulnerability
https://scm.hiwin.tw/ SCM	Medium	1/1	Weak cipher suitesupported (Will be patched on 11/30)
	Medium	1/0	Error message is too detailed (Patched)
	Medium	1/0	Unrestricted Upload of File (Patched)
https://vpn.hiwin.tw/ GlobalProtect Portal	Medium	1/0	Weak cipher suite supported (Patched)
https://www.hiwin.tw/ HIWIN Technologies Corp. Official Website	Medium	1/0	Support for deprecated SSL/TLS protocols (Patched)
	Medium	1/1	Weak cipher suite supported (Will be patched on 11/30)
	Medium	1/0	Enumerable user account (Patched)
	Medium	1/0	Session fixation (Patched)
	Medium	1/0	Captcha reuse (Patched)
	Medium	1/0	Error message is too detailed (Patched)

Target	Severity	Number (FT/RT)	Vulnerability
	Low	1/0	Session Cookie has no Secure attribute set (Patched)
https://hcrm.hiwin.tw/crm HCRM	Medium	1/0	Weak cipher suite supported (Patched)
mail.hiwin.tw Mail	Medium	1/0	No SMTP Authentication (Patched)

3. Penetration Testing Execution Results

Table 6 Execution Items and Results for this Project

Testing Type	Testing Category	Description	Result
Operating System	Remote Service	Contains at least remote service package vulnerability test.	Pass
	Local Service	Under the condition of getting privilege, contains at least a local machine package vulnerability test.	Pass
Web Service	Setting Management	Contains at least web application setting test, file type handling test, web site file crawling test, backend admin interface test, and HTTP protocol test.	Will be patched on 11/30
	User Authentication	Contains at least checking encryption transfer of sensitive data, user account enumeration, and so forth.	Pass
	Session Management	Contains at least session management test, cookie attribute test, session state renewal test, session variable transfer test, CSRF test, and so forth.	Pass
	User Authorization	Contains at least path privilege test, authorization mechanism test, access control mechanism test, and so forth.	Pass
	Logic Vulnerability	Contains at least web application function test, web function design missing test, file upload test, and so forth.	Pass
	Input Validation	Contains XSS Injection test, SQL Injection test, LDAP Injection test, XML Injection test, SSI Injection test, XPath Injection test, Code Injection test, OS Command Injection test, bogus HTTP method test, and so forth.	Pass
	Web Service	Contains at least WSDL test, XML structure test, XML content test, XML parameter transmission test, and so forth.	Pass
	Ajax	Contains at least Ajax vulnerability test such as missing settings, access control package weakness, and so forth.	Pass

Testing Type	Testing Category	Description	Result
Application	Email Service Package	Contains at least some common external Email services, SMTP, POP3 and IMAP, such as missing settings, access control ， package weakness, and so forth.	Pass
	Web Service Package	Contains the common WEB package vulnerability test such as missing settings, access control, package weakness, and so forth.	Pass
	File Transfer Service Package	Contains at least some common file transfer services, FTP, NETBIOS, and NFS, such as missing settings, access control and package weakness, and so forth.	Out of Scope
	Remote Connection Service Package	Contains at least some common remote connection service, SSH, TELNET, VNC, and RDP, such as missing settings, access control, package weakness, and so forth.	Out of Scope
	Internet Service Package	Contains at least some common internet services, DNS, PROXY, and SNMP, such as missing settings, access control, package weakness, and so forth.	Out of Scope
	Others	Contains at least some common application or internet package, Firewall, Database, LDAP, SMB, LPD, IPP, Jetdirect, RTSP and so forth.	Out of Scope
Password Cracking	Password Strength Test	Contains at least WEB, FTP, SSH, TELNET, SMTP, POP3, IMAP, SNMP, NetBIOS, RDP, VNC, and Database password dictionary attack. Wi-Fi password dictionary attacks can be carried out under onsite service conditions.	Pass
Wireless Service	Wireless Service Vulnerability Test	Wireless service package vulnerability test can be carried out under onsite service conditions.	Out of Scope

Project Plan

1. Execution Period and Duration

   The testing effort took place from 2024/09/27 to 2024/09/30. The test can be performed in principle 24 hours a day at any time during the execution phase unless the client has specifically excluded the testing time limit. Basically, our principle is to carry out 8 hours per person per day.

2. Execution Details

   (1) Risk Management and Assessment

   To prevent situations such as unexpected damage or loss of information, we suggest backing up the tested targets before the penetration test execution.

   During the penetration test execution, no intrusive testing operations will be performed until both parties have discussed the appropriate timing and established proper contingency measures and risk assessments.

   Due to project schedule constraints, the testing team is responsible for identifying the most exploitable vulnerabilities within a limited timeframe but cannot guarantee absolute system safety or the absence of entry points.

   Penetration test is based on utilizing the shortest path to penetration rather than detecting all possible penetration paths. If exploitable vulnerabilities are discovered during the execution, penetration will be conducted following analysis.

   (2) Methodology

   A. ISECOM（Institute for Security and Open Methodologies）：OSSTMM（Open Source Security Testing Methodology Manual）v3.0

   B. OWASP（Open Web Application Security Project）：WSTG（Web Security Testing Guide）v 4.2

   (3) Explanation of Penetration Testing Detection Process