C008 Certification Report
MecWise eHuman Resource 3.1 R1

File name: MyCB-5-RPT-C008-CR-v1
Version: v1
Date of document: 5 October 2010
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

C008 Certification Report
MecWise eHuman Resource 3.1 R1

5 October 2010

MyCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8946 0999 Fax: +603 8946 0888
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C008 Certification Report - MecWise eHuman Resource 3.1 R1
DOCUMENT REFERENCE:	MyCB-5-RPT-C008-CR-v1
ISSUE:	v1
DATE:	5 October 2010

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:
Level 8, Block A,
Mines Waterfront Business Park,
No 3 JalanTasik, The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Printed in Malaysia

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) established within CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 28 October 2010, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	5 October 2010	All	Final Released.

Executive Summary

The MecWise eHuman Resource 3.1 R1 (hereafter referred as MecWise HR 3.1 R1) from Starvision Information Technology Sdn. Bhd. is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE is software that comprises of:

- MecWise eHuman Resource 3.1 R1, a web based application that facilitates recording, tracking, retrieving, reporting and maintaining of Employee Profile Information, and
- MecWise Audit Trail Utility 1.0 application that provides the ability to enable/disable audit function, view and filter transactions log events.

The modules of the TOE that are within the scope of the evaluation include Security Profile, Security Group, User Account Profile, Session Log Viewer, Audit Trail Utility, and Web Interface.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for MecWise HR 3.1 R1, the security requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of MecWise HR 3.1 R1 to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the product has met the target assurance level of EAL1 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the CyberSecurity Malaysia MySEF and was completed on 20 September 2010.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the MecWise HR 3.1 R1 evaluation meets all the conditions of the MyCC Scheme requirements and that the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the MecWise HR 3.1 R1 meets their requirements. It is recommended that a potential user of the MecWise HR 3.1 R1 to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

1 Target of Evaluation 1

1.1 TOE Description 1

1.2 TOE Identification 1

1.3 Security Policy 2

1.4 TOE Architecture 2

1.4.1 Logical Boundaries 2

1.4.2 Physical Boundaries 3

1.5 Clarification of Scope 4

1.6 Assumptions 5

1.6.1 Usage assumptions 5

1.6.2 Environment assumptions 5

1.7 Evaluated Configuration 5

1.8 Delivery Procedures 6

1.9 Documentation 6

2 Evaluation 7

2.1 Evaluation Analysis Activities 7

2.1.1 Life-cycle support 7

2.1.2 Development 7

2.1.3 Guidance documents 7

2.1.4 IT Product Testing 7

3 Results of the Evaluation 13

3.1 Assurance Level Information 13

3.2 Recommendation 13

Annex A References 15

A.1 References 15

A.2 Terminology 15

A.2.1 Acronyms 15

A.2.2 Glossary of Terms 16

. Index of Tables

Table 1: TOE identification 1

Table 2: Independent Functional Testing 8

Table 3: Evaluator's Penetration Testing Summary 10

Table 4: List of Acronyms 15

Table 5: Glossary of Terms 16

Index of Figures

Figure 1: TOE Logical Scope 2

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), MecWise HR 3.1 R1, is a human resource application which is a combination of web based and windows based (utility) application. The TOE comprises of:

a) MecWise eHuman Resource 3.1 R1, a web based application that facilitates recording, tracking, retrieving, reporting and maintaining of Employee Profile Information, and

b) MecWise Audit Trail Utility 1.0 application that provides the ability to enable/disable audit function, view and filter transactions log events.

1.2 TOE Identification

2 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C008
TOE Name	MecWise HR 3.1 R1
TOE Version	3.1 R1
Security Target Title	MecWise HR 3.1 R1 Security Target
Security Target Version	v1.11
Security Target Date	4 September 2010
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	**Starvision Information Technology Sdn. Bhd.** S28A, Jalan SS21/58, Damansara Utama, 47400, Petaling Jaya, Selangor Darul Ehsan

Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

3 MecWise HR 3.1 R1 implements access control security policy to a group of user to restrict the ability to add, query, modify, delete and print on other MecWise HR 3.1 R1 modules. The details of the access control security policy are described in Section 6 of the Security Target (Ref [6]).

4 The MecWise HR 3.1 R1 administrator is required to configure the policy rules for the access control security policy using the Security Group module interface. This policy rules is user definable based on their own organisation IT policy.

1.4 TOE Architecture

5 MecWise HR 3.1 R1 includes both logical and physical boundaries.

1.4.1 Logical Boundaries

6 Figure 1 below describes the components of MecWise HR 3.1 R1 that comprise the TOE; MecWise eHuman Resource 3.1 R1, a web based application, and MecWise Audit Trail Utility 1.0 application.

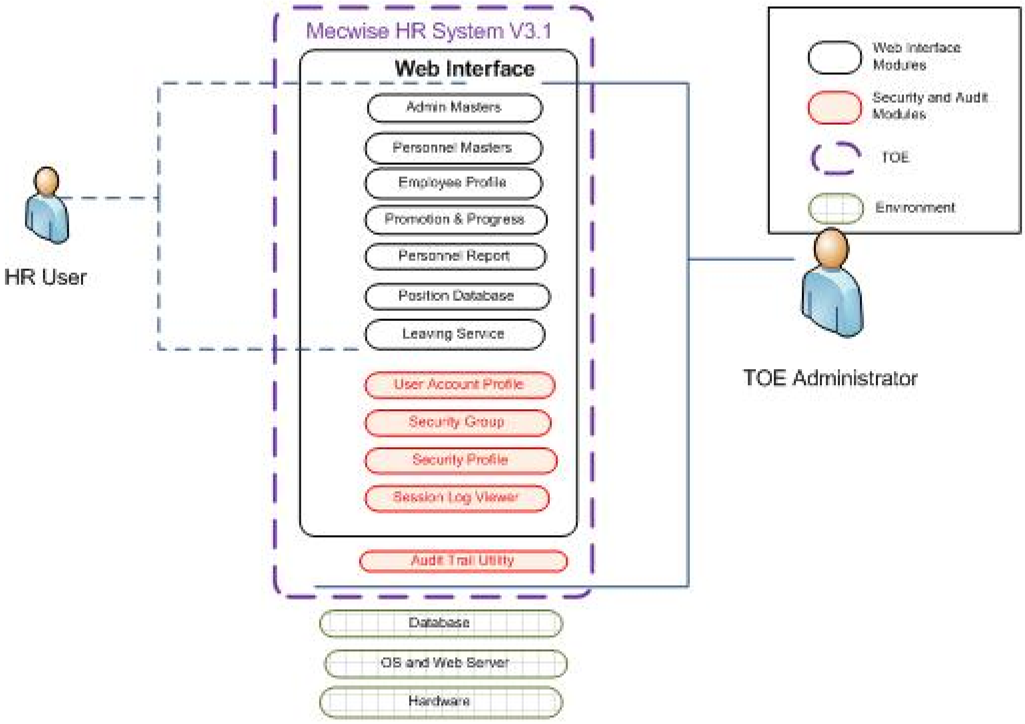

Figure 1: TOE Logical Scope

7 The TOE security modules comprise of the following:

a) **Web Interface** – Provides the interface to access all modules of the TOE except Audit Trail Utility module. Depends on the settings in Security Profile and Audit Trail Utility modules, actions that are performed on the web interfaces such as Opening of Screen, Adding a New Record, Deletion of record or Update of record, will trigger the creation of the session log or audit trail records and will be recorded in a table accessible by Session Log Viewer or Audit Trail Utility modules.

b) **Security Profile** – Enables management and configuration of security related user profiles. The security profiles also enables the generation of "session transactions events" via the Session Transaction Log.

c) **Security Group** – Enables creation and management of different security user groups to which access rights to web interface modules can be assigned. Ability to view, add, delete, modify record of a certain module which is user definable can also be managed from this module.

d) **User Account Profile** – Creation and management of users' security attributes such as user identification, password and password expiry control, controlling of modules accessible by a particular user based on the security user group.

e) **Session Log Viewer** – Provide the ability to view session logs of events such as screen open, screen record insertion, new password, screen record fetch, screen record update and screen record deletion.

f) **Audit Trail Utility** – provide the ability to enable or disable the TOE audit function. Enabling of Audit Trail feature will create an audit trail database table which have the similar structure of the original database table, and create correspond database trigger on the tables. Within the audit trail utility, the authorized administrator will be able to view and filter audit trail records.

8 Based on Figure 1, by default the TOE administrator can access all modules using the TOE Web Interface and audit trail from the Audit Trail Utility application. The TOE administrator is responsible to configure users' access based on the security group assigned to the user.

1.4.2 Physical Boundaries

9 Physically, the TOE is an application that requires a server with 1GHz or faster processor, operating system, web server, database and other supporting softwares as described in Section 1.2.2 of the Security Target (Ref [6]).

10 The Security Target assumes that any network connections, equipment, and cables are appropriately protected in the TOE security environment.

1.5 Clarification of Scope

11 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) **Audit Session Generations and Views** – provides the capability to generate audit trails and session logs performed by users through web interface. From the Audit Trail Utility, the administrator can enable or disable the TOE audit function. Administrator can also select the events to be logged such as screen open, screen fetch, screen delete, login, logout, and add data, for a user from Session Transaction Logs under the Security Profiles module. Authorised users can use Audit Trail Utility and Session Log Viewer module to query and view the audit trail and session log records;

b) **Identification and Authentication** – provides the means to ensure that the authorised users are authenticated to access the TOE via username and password. Username and password will be matched against the credentials created in User Account Profile module; and

c) **Security Management** – enables the authorised administrator to manage user's security attributes like username and password from the User Account Profile module, manage user's access rights from Security Group module, and managing the selection of events to be logged from Security Profile module

of MecWise eHuman Resource 3.1 R1 web application, and MecWise Audit Trail Utility 1.0 application.

12 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

13 Functions and services which are not included as part of the evaluated configuration are as follows:

a) MecWise User License Manager Utility software;

b) A Hardware Server;

c) An Operating System on which the TOE is installed on;

d) A Database Software on which the TOE is dependent on as its database;

e) Microsoft Internet Information Services 6.0 Web Server;

f) Other supporting software;

   i) Microsoft .NET Framework Version 2.0

   ii) Microsoft Windows Installer Version 3.1

   iii) Microsoft XML Core Services (MSXML) Version 4.0

   iv) Microsoft Data Access Components Version 2.8

v) A Web Browser known as Microsoft Internet Explorer Version 7

vi) SDA Client Installer Version 1 – (Pre-requisite third party software to be distributed together with the TOE during installation of TOE).

1.6 Assumptions

14 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the MecWise HR 3.1 R1 as defined in subsequent sections and in the Security Target.

1.6.1 Usage assumptions

15 This evaluation was performed at EAL1. Therefore, no assumption for the TOE usage was provided for the TOE.

1.6.2 Environment assumptions

16 Assumptions for the TOE environment listed in the Security Target are:

a) The TOE must be installed in a physically secured location to prevent attacker from accessing the TOE physically.

b) Person responsible of the TOE must ensure the TOE and any hardware/software/firmware required by TOE are delivered, installed, managed and operated in a secure manner.

c) The TOE administrator and users must ensure that the password is hard to guess.

d) The TOE administrator and users must ensure that the credentials of username and password are kept securely.

e) The TOE must be operated without access to Internet.

1.7 Evaluated Configuration

17 The TOE is to be configured according to the Preparative User Guidance (Ref 23a)).

18 The TOE is delivered as an application by the developer and developer will make changes to configuration based on Preparative User Guidance (Ref 23a)) as following:

a) Website Deployment

b) Web Server configuration

c) Report Server configuration

d) Database Server configuration

e) Audit Trail Utility configuration

1.8 Delivery Procedures

19 MecWise HR 3.1 R1 is delivered to the user by the developer's authorised personnel.

20 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process. In security objectives of the operational environment in Security Target (Ref [6]), OE_RESPONSIBILITY stated that the person responsible of TOE must ensure that the TOE and any hardware/software/firmware required by the TOE are delivered, installed, managed and operated in a secure manner. Therefore, the evaluators relied on the environment to provide a secure TOE delivery process.

1.9 Documentation

21 To ensure continued secure usage of the product, it is important that the MecWise HR 3.1 R1 is used in accordance with guidance documentation.

22 The following documentation is provided by the developer to the end user as guidance to ensure secure operation of the product:

a) MecWise HR V3.1 Operation Guide for Users, version 3.4, 18 May 2010

b) MecWise Human Resource Version 3.1 Security Guide for Users, version 3.5, 21 May 2010

23 The following documentation is used by the developer's authorised personnel as guidance to ensure secure installation of the product:

a) MecWise HR 3.1 Security Preparative User Guidance, version 1.4, 22 June 2010

2 Evaluation

24 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

25 The evaluation activities involved a structured evaluation of MecWise HR 3.1 R1, including the following components:

2.1.1 Life-cycle support

26 An analysis of the MecWise HR 3.1 R1 configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

2.1.2 Development

27 The evaluators analysed the MecWise HR 3.1 R1 functional specification; they determined that the document completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

28 The evaluators examined the MecWise HR 3.1 R1 preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

29 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The MecWise HR 3.1 R1 testing was conducted at CyberSecurity Malaysia MySEF where it was subjected to an independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Independent Functional Testing

30 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

31 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Five independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

TEST TITLE	DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
TEST GROUP A	Comprises a series of test cases on TOE security function to view audited event in each web interface. This includes: • HR modules • Security modules • Opening of screen • Fetching of screen	Audit Session Generations and Views	• Session Log Viewer (FAU_SAR.1.1, FAU_SAR.1.2, FPT_STM_EXT.1.1) • Web Interface (FAU_GEN.1.1, FAU_GEN.1.2)	Pass
TEST GROUP B	Comprises a series of test cases on TOE security functions of web based for the administrator to configure and manage the TOE. The test will cover: • Identification and authentication management • User and role management • Security management	• Identification and Authentication • Security Management	• Security Profile (FMT_SAE.1.1, FMT_SAE.1.2, FAU_SEL.1.1, FPT_STM_EXT.1.1) • Security Group (FMT_MOF.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_SMR.1.1, FMT_SMR.1.2, FMT_SMF.1.1, FMT_MTD.1.1, FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4) • User Account Profile (FIA_ATD.1.1, FMT_SMF.1.1, FMT_REV.1.1,	Pass

TEST TITLE	DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
			FMT_REV.1.2)	
TEST GROUP C	Comprises a series of test cases on TOE security functions of audit records generation for relevant authentication and management events such as: • Adding a New Record • Deletion of record • Update of record	Audit Session Generations and Views	• Audit Trail Utility (FAU_SAR.1.1, FAU_SAR.1.2, FAU_SEL.1.1, FPT_STM_EXT.1.1) • Security Group (FMT_MOF.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_SMR.1.1, FMT_SMR.1.2, FMT_SMF.1.1, FMT_MTD.1.1, FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4)	Pass
TEST GROUP D	Comprises a series of test cases by doing negative testing onto the TOE security function. This includes: • Authentication and identification management • Account management	Identification and Authentication Security Management	• Security Profile (FMT_SAE.1.1, FMT_SAE.1.2, FAU_SEL.1.1, FPT_STM_EXT.1.1) • Security Group (FMT_MOF.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_SMR.1.1, FMT_SMR.1.2, FMT_SMF.1.1, FMT_MTD.1.1, FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4) • User Account Profile (FIA_ATD.1.1, FMT_SMF.1.1, FMT_REV.1.1, FMT_REV.1.2)	Pass

TEST TITLE	DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
TEST GROUP E	Comprises a series of test cases to know the restriction in HR module and security attribute can only be configured in security module.	Identification and Authentication	User Account Profile (FIA_ATD.1.1, FMT_SMF.1.1, FMT_REV.1.1, FMT_REV.1.2)	Pass

32 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Penetration Testing

33 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, and functional specification.

34 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, to attack performed by an attacker possessing a basic attack potential.

35 The penetration tests focused on:

a) Compromising the TOE environment configuration; and

b) Hacking web application and server.

36 The vulnerabilities identified and tests conducted by the evaluator are listed in the following table:

Table 3: Evaluator’s Penetration Testing Summary

TEST TITLE	DESCRIPTION	VULNERABILITIES EXPLOITABLE	TEST STATUS
Vulnerability Test 1: OS password resetting	Accessing TOE server by resetting Windows 2003 password.	By enforcing OE_PHYSICAL to the operational environment, TOE must be installed in a physically secured location to prevent attacker from accessing the TOE physically. Therefore, this vulnerability is not exploitable in its operational environment.	Not Exploitable in TOE operational environment
Vulnerability Test 2: Password sniffing	Gather information that is crucial to the TOE. For example, username and password by using sniffer.	It is declared in the Security Target (Ref [6]) that the TOE will only be accessible directly by administrator and user without access to Internet. By enforcing OE_RESPONSIBILITY, person responsible of TOE must	Not Exploitable in TOE operational environment

TEST TITLE	DESCRIPTION	VULNERABILITIES EXPLOITABLE	TEST STATUS
		ensure TOE managed and operated in a secure manner. Therefore, this vulnerability is not exploitable in its operational environment.	
Vulnerability Test 3: Upload attack	Upload suspicious application into TOE server by using upload file function in TOE.	By enforcing OE_RESPONSIBILITY, person responsible of TOE must ensure TOE managed and operated in a secure manner. Therefore, this vulnerability is not exploitable in its operational environment.	Not Exploitable in TOE operational environment
Vulnerability Test 4: Cookies manipulation	Escalate normal user's privilege to administrator privilege by editing cookie value in user account.	By enforcing OE_RESPONSIBILITY, person responsible of TOE must ensure TOE managed and operated in a secure manner. Therefore, this vulnerability is not exploitable in its operational environment.	Not Exploitable in TOE operational environment
Vulnerability Test 5: SQL injection	Gather critical information occurring in database layer of an application by injecting SQL command.	None	Not Exploitable in TOE operational environment
Vulnerability Test 6: DOS attack	Prevent legitimate users from accessing TOE via DOS attack	None	Not Exploitable in TOE operational environment
Vulnerability Test 7: Password Brute Force attack	Brute force web authentication type form-based (password)	None	Not Exploitable in TOE operational environment

2.1.4.3 Testing Results

37 Tests conducted for the MecWise HR 3.1 R1 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

38 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential. However, the evaluators discovered potential vulnerability that is beyond basic attack potential and exceed AVA_VAN.1 requirement. These vulnerabilities to the TOE required additional resource, higher windows

opportunity, longer duration to exploit, higher skill/knowledge and focused tools to be exploited.

39 The residual vulnerabilities are:

a) **OS password resetting**: Without enforcing OE_PHYSICAL to the operational environment, TOE will not be installed in a physically secured location to prevent attacker from accessing the TOE physically. Therefore, this vulnerability is exploitable without its secure operational environment with higher windows of opportunity.

b) **Password sniffing**: Without enforcing OE_RESPONSIBILITY, person responsible of TOE will not ensure TOE managed and operated in a secure manner. Therefore, this vulnerability is exploitable without its secure operational environment with higher windows of opportunity.

c) **Upload attack**: Without enforcing OE_RESPONSIBILITY, person responsible of TOE will not ensure TOE managed and operated in a secure manner. Therefore, this vulnerability is exploitable without its secure operational environment with higher windows of opportunity.

d) **Cookies manipulation**: Without enforcing OE_RESPONSIBILITY, person responsible of TOE will not ensure TOE managed and operated in a secure manner. Therefore, this vulnerability is exploitable without its secure operational environment with higher windows of opportunity.

e) **DOS attack**: With longer duration and additional resource to send hping command to the TOE, it is anticipated that TOE will be in denial of service state.

3 Results of the Evaluation

40 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of MecWise HR 3.1 R1 performed by the CyberSecurity Malaysia MySEF.

41 The CyberSecurity Malaysia MySEF found that MecWise HR 3.1 R1 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

42 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

43 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

44 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

45 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

46 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

47 In addition to ensure secure usage of the product, below are additional recommendations for MecWise HR 3.1 R1 consumers:

a) Use the product only in its evaluated configuration;

b) HTTPS is recommended to be deployed in TOE environment by the server to ensure that the communication between client and server is encrypted. By deploying HTTPS, residual vulnerabilities of password sniffing will be encountered;

c) HTTPS is also recommended in order to prevent cookies tampering by cookies encryption. By deploying HTTPS, residual vulnerabilities of cookies manipulation will be encountered;

d) By enforcing a filter in user input field is also recommended to avoid user from uploading suspicious file to TOE server. By deploying this filter, residual vulnerabilities of upload attack will be encountered;

e) OS password resetting residual vulnerability is mitigated by the secure environment of the TOE which is the operating system (OS). The OS is expected to protect the TOE from attacker that use the OS interface as a medium for getting unauthorized access to the TOE; and

f) DOS attack residual vulnerability is mitigated by the secure environment of the TOE. Several options can be deployed:

   i) OS and network hardware/software are upgraded to the latest version.

   ii) install an Intrusion Prevention System (IPS) on gateway.

   iii) Implement white-list filtering on network firewall. This is to allow only data-traffic from/to certain (ranges of) IP addresses.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] MecWise HR 3.1 R1 Security Target, Version 1.11, 4 September 2010

[7] Evaluation Technical Report MecWise HR 3.1 R1, Version 1.2, 20 September 2010

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

Term	Definition and Source
MyCB Personnel	Includes all members of the Certification Subcommittee, the Scheme Manager, the Senior Certifier, Certifiers and the Quality Manager.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---