CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

# C013 Certification Report
# VirtualEye v5.0

File name: ISCB-5-RPT-C013-CR-v1a
Version: v1a
Date of document: 8 March 2011
Document classification: PUBLIC


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

# C013 Certification Report
# **VirtualEye v5.0**

8 March 2011
ISCB 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:*** | C013 Certification Report - VirtualEye v5.0 |
| ***DOCUMENT REFERENCE:*** | ISCB-5-RPT-C013-CR-v1a |
| ***ISSUE:*** | v1a |
| ***DATE:*** | 8 March 2011 |

| | |
|---|---|
| ***DISTRIBUTION:*** | UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION |

# Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2011

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) Unit, a unit established within Information Security Certification Body (ISCB) Department, 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 8 March 2011, 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 | 22 February 2011 | All | Final Released |
| v1a | 8 March 2011 | Page iv | Add the date of the certificate. |

# Executive Summary

The VirtualEye v5.0 from Viewtech International Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

VirtualEye v5.0 is a system designed to enable users to access live video camera feed or playback recorded video clips from the web portal or mobile devices.

The TOE comprises of 2 components:

- VirtualEye v5.0 Web portal, available for authorized subscribers and administrators, and
- VirtualEye v5.0 Mobile device application, for authorized subscribers. The TOE only covers those subscribers who are connected via Wi-Fi connectivity.

The functions of the TOE that are within the scope of evaluation covering the management of the security features which involves generate and view of audit log, validation of input field, user authentication and identification, add/edit/delete user account, add/edit/change user password and login session management for web portal.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for VirtualEye v5.0, 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 VirtualEye v5.0 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 18 November 2010.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the VirtualEye v5.0 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 VirtualEye v5.0 meets their requirements. It is recommended that a potential user of the VirtualEye v5.0 to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase and deploy the product.

# Table of Contents

# Index of Tables



# Index of Figures

# 1 Target of Evaluation

## 1.1 TOE Description

1 VirtualEye v5.0 is a system designed to enable users to access live video camera feed or playback recorded video clips from the web portal or mobile devices. The TOE comprises of:

a) VirtualEye v5.0 web portal available for authorized subscribers and administrators. Authorized subscribers and administrators access the web portal through their web browser over the Internet or within the LAN (for authorized administrators only). Live and recorded streaming of videos for subscribers are not part of the TOE, and

b) VirtualEye v5.0 Mobile application available for authorized subscribers. Authorized subscribers access the mobile application using a Wi-Fi connection. The subscribers can authenticate themselves using username and password through the mobile application.

## 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** | C013 |
| **TOE Name** | VirtualEye v5.0 |
| **TOE Version** | v5.0 |
| **Security Target Title** | VirtualEye Version 5.0 Security Target (EAL1) |
| **Security Target Version** | v6.7 |
| **Security Target Date** | 28 October 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<br>CC Part 3 Conformant<br>Package conformant to EAL1 |
| **Sponsor and Developer** | Viewtech International Sdn Bhd |

| | |
|---|---|
| | No.1 and 2 GM,<br>Jalan Pantai Cahaya ½,<br>Pandan Cahaya,<br>68000 Ampang,<br>Selangor Darul Ehsan.<br>Tel: 603 - 42702288<br>Fax: 603 - 42703668 |
| **Evaluation Facility** | CyberSecurity Malaysia MySEF |

## 1.3 Security Policy

3 VirtualEye v5.0 implements Access Control Policy as follow:

a) Only authorized administrators can add/edit/change password of user, edit/delete subscribers' accounts, add/edit/delete dealers' accounts and viewing of audit log.

b) Only authorized subscribers able to change own password, reset own password and viewing of own user audit log.

4 The details of the security policy are described in Section 6 of the Security Target (Ref [6]).

## 1.4 TOE Architecture

5 VirtualEye v5.0 includes both logical and physical boundaries which are described in Section 2.3 of the Security Target (Ref [6]).

### 1.4.1 Logical Boundaries

6 below describes the components of VirtualEye v5.0 that comprises the TOE;

7 Figure 1 below describes the components of VirtualEye v5.0 that comprises the TOE;

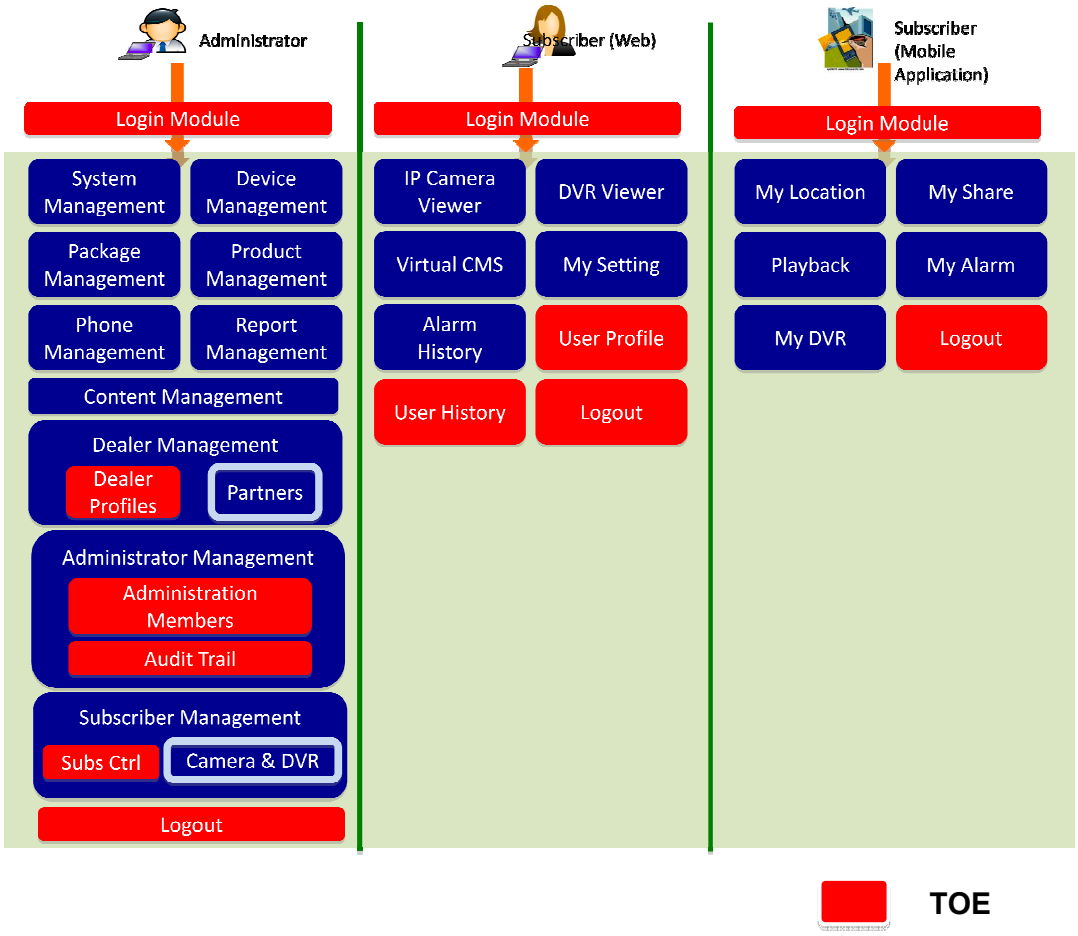


Figure 1: TOE Logical Scope

8 The TOE modules can be divided into 3 category, modules accessed by administrator through web application, modules accessed by subscriber through web application; and modules accessed by subscriber through mobile application. The TOE modules comprise of the following:

a) **Web application for administrator:**

i) **Administration Members:** Module used by administrator to manage list of administrator and users including add/edit administrator password, delete administrator account.

ii) **Subscriber Control:** Module used by administrator to manage list of subscriber including add/edit/delete subscribers' account.

iii) **Dealer Profiles:** Module used by administrator to manage list of dealers for Viewtech International Sdn Bhd including add/edit/delete dealers' account.

iv) **Login/Logout:** Module that controls administrator user access for login and logout from the TOE, logout will end the session and clears the cookies for that administrator's session.

v) **Audit Trail:** Module used by administrator to view audit log.

b) **Web application for subscriber:**

i) **User Profile:** Module used by subscriber to manage or update personal information about his own subscription including change own password or reset own password.

ii) **User History:** Module used by subscriber to view the audit trail of his own activities.

iii) **Login/Logout:** Module that controls subscriber user access for login and logout from the TOE, logout will ends the session and clears the cookies for that subscriber's session.

c) **Mobile application for subscriber:**

i) **Login/Logout:** Module that controls subscriber user access for login and logout from the TOE, logout will ends the session and clears the cookies for that subscriber's session.

### 1.4.2 Physical Boundaries

9 Physically, the TOE comprises of a web application that requires a recording and streaming server, email server and web server with 3.0Ghz/2M, 800MHz processor, database server with 3.4Ghz/2M, 800MHz processor, operating system, database software, client machine with at least 1GHz processor, mobile phones that support Java and Wi-Fi enabled and other supporting softwares as described in Section 2.2.2 of the Security Target (Ref [6]).

10 The Security Target assumes that the server is to be located in a secure area that is free from physical access to unauthorised parties.

## 1.5 Clarification of Scope

11 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communication security in accordance with administrator guidance that is supplied with the product.

12 Figure 1 in Section 1.4.1 of this document shows the scope of the evaluation. 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) **Security Audit** – The Audit Trail module generates audit logs that consist of various auditable events or actions. Date and time of events, IP addresses, usernames, and modules accessed, and events or actions taken by the authorized users are recorded.

   i) Authorized administrators have the capability to read and view all the recorded logs for administrative accounts through the web portal. The audit trail generated is able to relate activities and events taken place to the specific usernames which then can be traced to the specific defined roles.

   ii) Authorized subscribers can view their own history of activities via a web browser in the User History sub-module within the Web Portal. They are able to view the event ID, task category, detail task, date / time, and the IP address.

b) **User Data Protection** – Input field available in the interactive forms in the VirtualEye v5.0 Web Portal is validated before it is processed. The input validation is performed for the web subscriber login form (both username and password fields). The input is validated based on the list of unacceptable characters (known as “black” list) to ensure that no malicious code is inserted into the SQL query.

c) **Identification and Authentication** – The TOE requires users (administrator and subscriber) to be identified and authenticated by means of username and password prior to performing any actions. Authorized subscriber is only restricted to only view their own data. A minimum of 6 and maximum of 12 characters is required for the passwords. In the case of user forgot his password, the user have to click the “Forgot Password” button and enter the username and email address to receive a new password from the system via email. The new password will be auto generated using Automatic Random Password Generator (ARPG). CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) will be used in the “Forgot Password” page and in user profile page to ensure all the forms are fill in by human being instead of Spybot.

d) **Security Management** – There are 2 roles of user maintained in TOE; subscriber and administrator. Each role can performed several security management functions.

   i) Authorized administrators can perform the following functions:

   (a) Add, edit, change passwords or delete administrative accounts in the Administration Members sub-module.

(b) Edit or delete subscribers' accounts in the Subscriber Control (Subs Ctrl) module.

(c) Add, edit, or delete dealers' accounts in the Dealer Profiles module.

(d) View administrative logs in the Audit Trail module.

ii) Authorized web-based subscribers can perform the following functions:

(a) Change own password in the User Profile sub-module.

(b) Reset password via the usage of ARPG.

(c) View own user history or logs in the User History sub-module.

e) **TOE Access** – Web portal has a session management function which is timeout function. The default session timeout is 10 minutes. This security function is only available for the sessions established via the web portal, not the mobile application.

13 The scope of evaluation covers networked and Internet (un-trusted network) environment. Authorized administrators can access the TOE from the Internet or within the LAN. Authorized subscribers can access the TOE from the Internet. Authorized subscribers also can access the mobile application through Internet using standard communication technology such as GPRS, EDGE, 3G, HSDPA and Wi-Fi connection. The TOE scope only covers those subscribers who are connected via **Wi-Fi** connectivity.

14 Live and recorded streaming of videos from the IP cameras and streaming/recording server are not part of the TOE.

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

a) A hardware server;

b) An operating system on which the TOE is installed on;

c) A database software on which the TOE is dependent on as its database;

d) Other supporting software;

i) Java-supported mobile phones; and

ii) Web browser.

## 1.6 Assumptions

16 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 VirtualEye v5.0 as defined in the Security Target.

17 However, there is no assumption declared by developer in the ST.

## 1.7 Evaluated Configuration

18 This section describes the configurations of the TOE that are included within the scope of the evaluation. The assurance gained via evaluation applies specifically to

the TOE in the defined evaluated configuration according to the Preparative User Guidance (Ref 27a)).

19 The VirtualEye v5.0 relevant software and hardware was installed at the developer's site. The developer's personnel installed the TOE and make changes to the configuration based on Preparative User Guidance (Ref 27a)) as following:

a) Installation and configuration of network architecture.

b) Installation and configuration of hardware.

c) Installation and configuration of web portal.

d) Installation and configuration of mobile application.

20 The only installation to be performed (in relation to the TOE) by the subscribers is the mobile application for their mobile phones. This installation package can be downloaded from VirtualEye v5.0 Web Portal by the subscribers.

## 1.8 Delivery Procedures

21 The VirtualEye v5.0 system is already installed and hosted at the developer's data centre. The only installation to be performed (in relation to the TOE) by the subscribers is the mobile application for their mobile phones. This installation package can be downloaded from the VirtualEye v5.0 Web Portal by the subscribers.

22 Authorized dealer is responsible to deliver the installation packages for the routers/modems, DVR players, and IP cameras to the subscribers. These installation packages belong to the manufacturers of those devices, not Viewtech International Sdn. Bhd. (the developer of the TOE).

23 The acceptance of the TOE is performed by the subscriber after a successful installation and testing. The checklist is provided as in Acceptance Checklist (Ref 27c)).**Error! Reference source not found.**

24 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.

## 1.9 Documentation

25 To ensure continued secure usage of the product, it is important that the VirtualEye v5.0 is used in accordance with guidance documentation.

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

a) VirtualEye v5.0 Operative Guidance, version 1.1, 28 October 2010.

b) User Manual for VirtualEye 5.0 Subscriber, version 1.2.

c) User Manual for VirtualEye 5.0 Admin, version 1.2.

d) User Manual for Subscribers (Mobile Application) version 1.0.

27 The following documentation is used by the authorized dealer and subscriber as guidance to ensure secure installation of the product:

a) VirtualEye v5.0 Preparative Guidance, version 1.3, 28 October 2010

b) VirtualEye v5.0 Installation Manual, version 2.1.

c) VirtualEye v5.0 Acceptance Checklist, version 1.2.

# 2 Evaluation

28 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

29 The evaluation activities involved a structured evaluation of VirtualEye v5.0, including the following components:

### 2.1.1 Life-cycle support

30 An analysis of the VirtualEye v5.0 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

31 The evaluators analysed the VirtualEye v5.0 functional specification; they determined that the design 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

32 The evaluators examined the VirtualEye v5.0 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

33 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The VirtualEye v5.0 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

34 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.

35 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

| DESCRIPTION | SECURITY FUNCTION | TSFI | TEST RESULT |
|---|---|---|---|
| This test group comprises a series of test cases on TOE security functions of web based for audit records generation for relevant authentication and management events. | Security Audit | Audit Trail<br>User History<br>Camera Setting | PASS |
| This test group comprises a series of test cases on TOE security functions of how TOE control access and privilege for each user. | User Data Protection | Subscriber and Administrator Login<br>Automated Random Password Generation | PASS |
| This test group comprises a series of test cases on TOE security functions of identification and authentication of administrator and subscriber through web portal and mobile application. | Identification and Authentication | Mobile Subscriber Page<br>Subscriber and Administrator Login<br>Administrator Logout<br>Web Subscriber Logout<br>Mobile Subscriber Logout<br>Input Validation<br>Automated Random Password Generation | PASS |
| This test group comprises a series of | Security | Administrator | PASS |

| DESCRIPTION | SECURITY FUNCTION | TSFI | TEST RESULT |
|---|---|---|---|
| test cases on TOE security functions of management function for administrator in web portal. | Management | Page<br>Web Subscriber Page<br>Administration Members<br>Dealer Profiles<br>Subscriber Control<br>User Profile | |
| This test group comprises a series of test cases on TOE security functions of monitoring user session in web portal. | TOE Access | Session Timeout | PASS |

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

#### 2.1.4.2 Penetration Testing

37 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.

38 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. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE;

d) Window of opportunity; and

e) IT hardware/software or other requirement required for exploitation.

39 The penetration tests focused on:

a) Generic vulnerabilities;

b) Bypassing;

c) Tampering; and

d) Direct attacks.

40 The results of the penetration testing note that there is no vulnerability or residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

#### 2.1.4.3 Testing Results

41 Tests conducted for the VirtualEye v5.0 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

# 3 Results of the Evaluation

42 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 VirtualEye v5.0 performed by the CyberSecurity Malaysia MySEF.

43 The CyberSecurity Malaysia MySEF found that VirtualEye v5.0 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.

44 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

45 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.

46 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.

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

## 3.2 Recommendation

48 In addition to ensure secure usage of the product, below are additional recommendations for VirtualEye v5.0 consumers:

a) Administrator and subscriber should follow closely the user manual for administrator (Ref [10]), user manual for subscriber (Ref [9]) and user manual for mobile application (Ref [8]) to ensure proper usage of the TOE .

b) Administrator of the TOE should ensure secure configuration and installation of supporting requirement of the TOE by closely following the installation manual (Ref [11]) provided by the developer.

# 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] VirtualEye Version 5.0 Security Target (EAL1), Version 6.7, 28 October 2010.

[7] Evaluation Technical Report VirtualEye v5.0, Version 1.1, 19 November 2010.

[8] User Manual for Subcribers (Mobile Application 5.0) Version 1.0.

[9] User Manual for VirtualEye 5.0 Subscriber, Version 1.2.

[10] User Manual for VirtualEye 5.0 Admin, Version 1.2.

[11] VirtualEye 5.0 Installation Manual version 2.1.

[12] VirtualEye Version 5.0 EAL 1 Acceptance Checklist, version 1.2.

## A.2 Terminology

### A.2.1 Acronyms

Table 3: 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 for Organisation |
| ISCB | Information Security Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |

| Acronym | Expanded Term |
|---|---|
| MySEF | Malaysian Security Evaluation Facility |
| PP | Protection Profile |
| ST | Security Target |
| TOE | Target of Evaluation |
| ARPG | Automated Random Password Generator |
| DVR | Digital Video Recorder |
| EDGE | Enhanced Data for Global Evolution is a third-generation, high-speed, mobile data and Internet access technology |
| FIPS PUB | Federal Information Processing Standards Publication |
| GB | Giga Bytes |
| GPRS | General packet radio service (GPRS) is a packet oriented mobile data service available to users |
| HSDPA | High-Speed Downlink Packet Access |

### A.2.2 Glossary of Terms

Table 4: 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 |

| Term | Definition and Source |
|---|---|
| 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. |
| 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 ---