VIEWSONIC
ON-SITE OBSERVATION REPORT

Security Verification and Validation Program

– Security Requirements Testing

Report n°: CYT- BCFD-WTW-Q231111501 **Written by Hans Hsieh**

This report contains 12 pages.

Bureau Veritas Consumer Products Services (Hong Kong) Limited,

Taoyuan Branch Mobile Communications Laboratory

**Avançons en confiance*

Move Forward with Confidence*

Table of content

1. VISAS AND REVISION HISTORY

Rev / Date	Witness Engineer	Technical Assessor	Content/ Reason
2023-11-16	Gill Chen	Hans Hsieh	First issue

VIEWSONIC Contact
Chan Chak Sum (Sam) | Cyber Security Manager Email: sam.cs.chan@VIEWSONIC.com

BUREAU VERITAS Contact
Hans Hsieh | Cybersecurity Technical Manager Email: hans.hsieh@bureauveritas.com

2. REFERENCES AND GLOSSARY

2.1 Manufacturer Documentation

Reference	Title
ID01	VIEWSONIC Secure Software Development Lifecycle.pdf
ID02	Network Testing Plan.docx
ID03	Android Testing Plan.docx
ID04	Windows Testing Plan.docx
ID05	Testing report of vCast_20231116.docx (MD5:db97a0c1040c8301b5fa3e6617b3d467) (SHA256:ba501cfe2e4ded9d31b4d6c22668fc309698dcb653f5e86e4e1164f071be52af)
ID06	VCastReceiver_v2.4.1114_4 in 1-3.apk_signed.apk
ID07	ID05 evidences of the network capture package files, including *Pcap1: 20231116-1038.pcapng (MD5: b254b18182d16acb97e520461eba6acd)* *Pcap2: 20231116-1109.pcapng (MD5: 086bcfe3325453254eaa7f9dbc705a84)* *Pcap3: 20231116-1140.pcapng (MD5: b4131643c8e9c922dbd1033ccf61fec5)* *Pcap4: 20231116-1210.pcapng (MD5: 3eefa8c4b635f438303bb1c161f2b0a1)*

Table 1 : Standards

2.2 Reference Standards

Reference	Title
IEC62443-4-1 Edition 1.0 2018-01	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Table 2 : References

2.3 Glossary

Acronym	Meaning
OWASP	Open Web Application Security Project
MASVS	Mobile Application Security Verification Standard
SR	Security Requirement
SF	Security Function
SSDLC	Secure Software Development Lifecycle
ToE	Target of Evaluation
SW	Software

Table 3 : Acronyms

3. INTRODUCTION

3.1 Project Scope

This project is to evaluate that the manufacturer, VIEWSONIC, can implement software development activities "**Testing phase**" and to ensure that manufacturer verifies that all the security requirements have been met for the product and the security of the product is maintained when it is used in its product security context correctly.

VIEWSONIC security team provided the security development policy of "Secure Software Development Lifecycle (SSDLC)" which contains 6 phases shown as below to define process of creating software, and this project is focused on "**Testing phase**."

- Requirement analysis
- Planning
- Software Design
- Software Development
- **Testing**
- Deployment
- Maintenance

The evaluation methodology is referred to IEC62443-4-1 practice 5 Security verification and validation testing, SVV1 Security requirement testing.

- Practice 5 Security verification and validation testing:
    - SVV1 Security requirement testing:

      A process shall be employed for verifying that the product security functions meet the security requirements and that the product handles error scenarios and invalid input correctly, like as functional testing of security requirements.

4. Evaluation Overview

The objectives of this project are described as followed:

1) Review the VIEWSONIC documentation, including SSDLC policy and procedure, the security function test cases, and the test report.

2) An on-site witness phase is performed to check the "**Testing Phase**" employed for verifying the product security functions meet the security requirements.

3) Once evaluation is completed and the observation report is deliveries.

The following listed two task items had been established to provide more detailed information of the evaluation activities.

- **Task 1: Document Analysis :**
    - Examination of evidence provided by manufacturer.
    - Creation of an open points list if required.
- **Task 2: On-site Witness :**
    - BV visited to VIEWSONIC premises to witness security requirement tests based on security verification and validation program for three test cases from the VIEWSONIC SSDLC requirements.

4.1 Evaluation team

The Witness activity has been performed by those following Bureau Veritas Team Members:

- Evaluator n°1: Hans Hsieh — Cybersecurity Technical Manager
- Evaluator n°2: Gill Chen — Cybersecurity Senior Engineer
- Field Support n°3: Joseph Chan — Cybersecurity Project Supervisor

5. Task 1: Document analysis

5.1 Security Team Positions

According ID01, the statement from VIEWSONIC indicated the **security team R&R** as below:

> Security team is willing to co-work with different teams to protect our product. Security team is not going to apply the old-fashioned security safe-guard way to the team. Our security team is going to achieve our security goal that protects all our products by the smooth adoption method.
>
> Security team also would help to handle all the security incidents, no matter it is related to data breaches, development process or hosting issue, security team could be helped on it.

5.1 Secure Software Development Lifecycle (SSDLC)

According ID01, the statement from VIEWSONIC indicated the **SSDLC** as below:

> SSDLC is the methodology with defined process of creating software. The processes could basically categorized tasks into 6 phases: Requirement analysis, Planning, Software Design, Software Development, Testing, Deployment, Maintenance.

5.2 Security Testing and Assessment

According ID01, the statement from VIEWSONIC indicated the **Security Testing** as below:

> Besides compliances, the security testing and assessments could be an important process to ensure the security for the products we develop Code Reviews, SAST, DAST, Vulnerability Scan

According ID02, ID03, and ID04 test plan created from VIEWSONIC security team, these are the security testing guidance on Android-based or Windows-based network devices such as vCast sender agent.

5.3 Evaluation Result

The VIEWSONIC security team is to lead the SSDLC program, and their aim is to support security management and ensure that the security-related activities are adequately planned, documented and executed throughout the product's life-cycle in an iterative pattern.

And BV observes that the VIEWSONIC security team, during **"Test Phase"**, did monitor that the security validation test plan must be created as well as that the general validation test plan must have a section for security.

6. Task 2: On-site Witness

A 5 hours on-site observation took place on Thursday November 16th of 2023.

The interview was conducted on VIEWSONIC in Taiwan.

The following participants attended the audit interview:

-------- Interviewees (VIEWSONIC): --------

- Sam Chan - Cyber Security Manager
- Tommy Tseng - Security Architect
- Dexter Chang - Security Engineer

-------- Interviewers (BV): --------

- Hans Hsieh — Cybersecurity Technical Manager
- Gill Chen – Cybersecurity Senior Engineer
- Joseph Chan – Cybersecurity Project Supervisor

<< Onsite visit the VIEWSONIC Testing Lab >>

6.2 Testing Phase

6.2.1 Verification Activities

Refer to IEC62443-4-1 practice 5 Security verification and validation testing, SVV1 Security requirement testing to verify the following items.

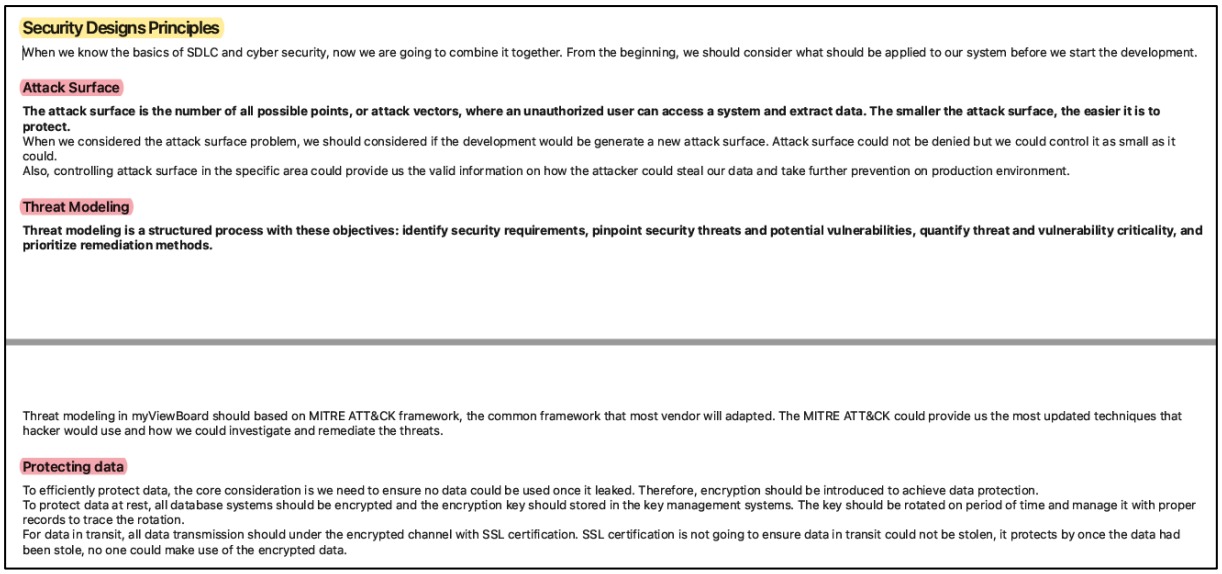
- **Verify that a security validation test plan is created**

Based on ID01 SSDLC policy and procedure, the security team had security requirement meeting to created three test case for vCast product.

Document ID	Test Case
ID02	Network Testing Plan
ID03	Android Testing Plan
ID04	Windows Testing Plan

- **Verify through sampling that all security requirements have test cases associated with them.**

Based on ID01 SSDLC policy and procedure, the security team had defined the security design principle and there are three topic required to meet, including Attack Surface, Threat Modeling, Protecting Data. And the on-site witness task is to observe the security requirement of protection data.



Security Designs Principles

When we know the basics of SDLC and cyber security, now we are going to combine it together. From the beginning, we should consider what should be applied to our system before we start the development.

Attack Surface

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect.
When we considered the attack surface problem, we should considered if the development would be generate a new attack surface. Attack surface could not be denied but we could control it as small as it could.
Also, controlling attack surface in the specific area could provide us the valid information on how the attacker could steal our data and take further prevention on production environment.

Threat Modeling

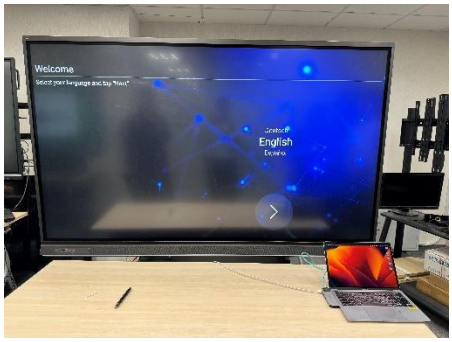
Threat modeling is a structured process with these objectives: identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.

Threat modeling in myViewBoard should based on MITRE ATT&CK framework, the common framework that most vendor will adapted. The MITRE ATT&CK could provide us the most updated techniques that hacker would use and how we could investigate and remediate the threats.

Protecting data

To efficiently protect data, the core consideration is we need to ensure no data could be used once it leaked. Therefore, encryption should be introduced to achieve data protection.
To protect data at rest, all database systems should be encrypted and the encryption key should stored in the key management systems. The key should be rotated on period of time and manage it with proper records to trace the rotation.
For data in transit, all data transmission should under the encrypted channel with SSL certification. SSL certification is not going to ensure data in transit could not be stolen, it protects by once the data had been stole, no one could make use of the encrypted data.

- **Verify that the validation results show that the plan was executed.**

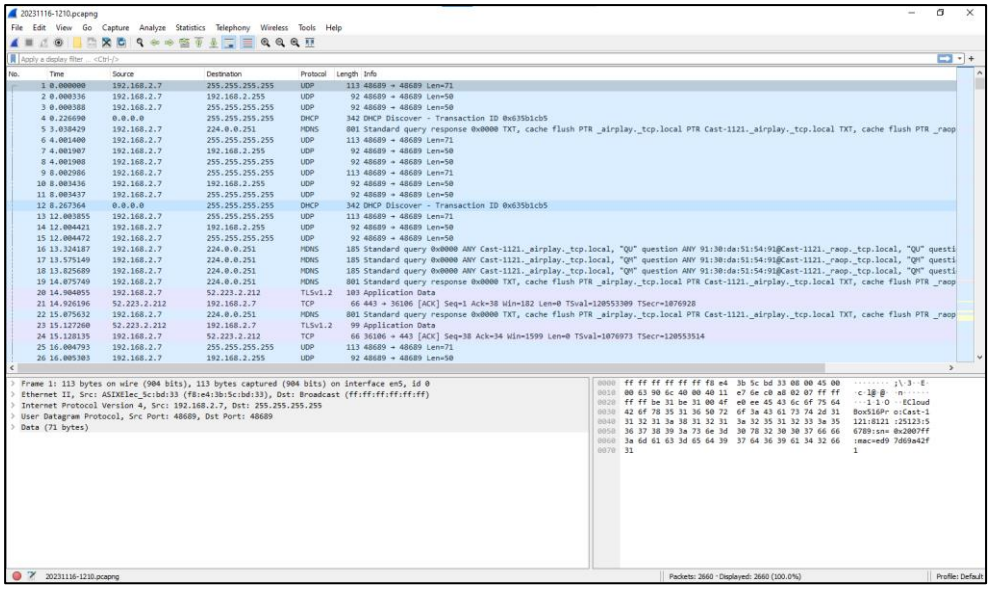


<< Testing environment setup: reset to factory setting >>

<< VIEWSONIC Cyber Security team was running the Network Testing Plan. >>

- **Verify that the validation results are documented.**

All test cases are performed and provided the ID05 VIEWSONIC Presentation Group vCast testing report and ID07 Wireshark capture network testing package files.



<< Network package analysis>>

- **Verify that this type of testing has been done on the product being evaluated by looking for evidence of (i) a completed checklist (ii) review meeting minutes showing that this was reviewed**

On-site witness is performed to participate the network package analysis meeting activities.

<< Review Meeting >>

- **Verify that this is done as a normal part of the process rather than in just one instance.**

Based on ID01 SSDLC policy and procedure, the security team had defined Secure Deployment, it is to ensure the deployment is secure enough, the regular testing on system is recommended.

- **Regular testing** could help us to know what had been happened and how we could reacts to the flaws.
- **Regular testing** not only providing the result on how we react, but also provide the score sheet to us about how well the product we developed.

Secure deployment

To ensure the deployment is secure, the pre-deployment scans is one of the method we can use.
In myViewBoard, Security Team is introducing the SAST and DAST process to ensure our product security is met the industrial standard which would provide the defense line for our deployment.
Besides, all colleagues is recommended to cross check teammates deployment machines which only need to consist the required packages only.
Also, to ensure the deployment is secure enough, the regular testing on system is recommended. Regular testing could help us to know what had been happened and how we could reacts to the flaws. Regular test not only providing the result on how we react, but also provide the score sheet to us about how well the product we developed.

7. Conclusion

7.1 Verdict after the observation

As demonstrated during the documentary analysis and on-site witness program, the VIEWSONIC security team has indeed create the SSDLC policy and procedure and we observe the primary goal of these security requirements is to align the security development process with the elevated security needs of product users against misuse or others.

The observation result is **POSITIVE** for the capability of SSDLC Teat Phase defined by VIEWSONIC security team.

7.2 Technical Advice

Refer to global best practice of security baseline for consumer device from ETSI EN 303 645 V2.1.1 (2020-06) Clause 6, please see details as below.

6 Data protection provisions for consumer IoT

Many consumer IoT devices process personal data. It is expected that manufacturers provide features within consumer IoT devices that support the protection of such personal data. In addition, there exist laws and regulations that relate to the protection of personal data in consumer IoT devices (for example the GDPR [i.7]). The present document intends to help manufacturers of consumer IoT devices provide a number of features for the protection of personal data from a strictly technical perspective.

Provision 6-1 The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

Provision 6-2 Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way. Obtaining consent "in a valid way" normally involves giving consumers a free, obvious and explicit opt-in choice of whether their personal data can be used for a specified purpose.

Provision 6-3 Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time. Consumers expect to be able to preserve their privacy by configuring IoT device and service functionality appropriately.

Provision 6-4 If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.

Provision 6-5 If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.