Secure Coding Lab Audit

# Vulnerability Report

Saturday, May 15, 2021

# MODIFICATIONS HISTORY

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 05/15/2021 | Shaik Vazeem | Initial Version |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

# General Information

## Scope

VIT VELLORE has mandated us to perform security tests on the following scope:

- Entire infrastructure

## Organisation

The testing activities were performed between 05/01/2021 and 05/15/2021.

# EXECUTIVE SUMMARY

# VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

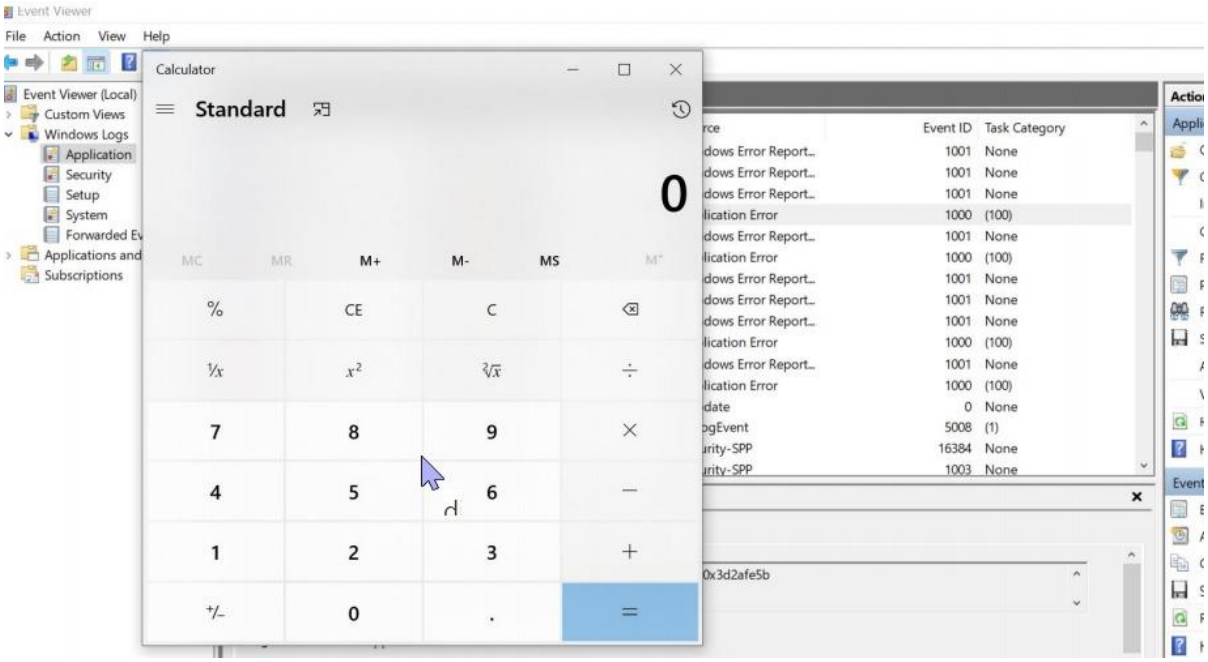
| Risk | ID | Vulnerability | Affected Scope |
|---|---|---|---|
| High | IDX-002 | Shell code injection | |
| High | IDX-001 | Buffer overflow | |
| High | IDX-003 | DOM XSS | |

# TECHNICAL DETAILS

## SHELL CODE INJECTION

| **CVSS SEVERITY** | **High** | | **CVSSv3 SCORE** | **8.9** |
|---|---|---|---|---|
| **CVSSv3**<br>**CRITERIAS** | Attack Vector :<br>Attack Complexity :<br>Required Privileges :<br>User Interaction : | **Network**<br>**Low**<br>**Low**<br>**Required** | Scope :<br>Confidentiality :<br>Integrity :<br>Availability : | **Changed**<br>**Low**<br>**High**<br>**High** |
| **AFFECTED SCOPE** | | | | |
| **DESCRIPTION** | Shell Code Injection is an attack that consists in executing commands on a victim's operating system via a vulnerable application. | | | |
| **OBSERVATION** | We have identified that this vulnerability can execute different malicious code and even trigger different application including command prompt. | | | |

**TEST DETAILS**



| rce | Event ID | Task Category |
|---|---|---|
| dows Error Report... | 1001 | None |
| dows Error Report... | 1001 | None |
| dows Error Report... | 1001 | None |
| lication Error | 1000 | (100) |
| dows Error Report... | 1001 | None |
| lication Error | 1000 | (100) |
| dows Error Report... | 1001 | None |
| dows Error Report... | 1001 | None |
| dows Error Report... | 1001 | None |
| lication Error | 1000 | (100) |
| dows Error Report... | 1001 | None |
| lication Error | 1000 | (100) |
| date | 0 | None |
| pgEvent | 5008 | (1) |
| urity-SPP | 16384 | None |
| urity-SPP | 1003 | None |

Image 1 – image.png

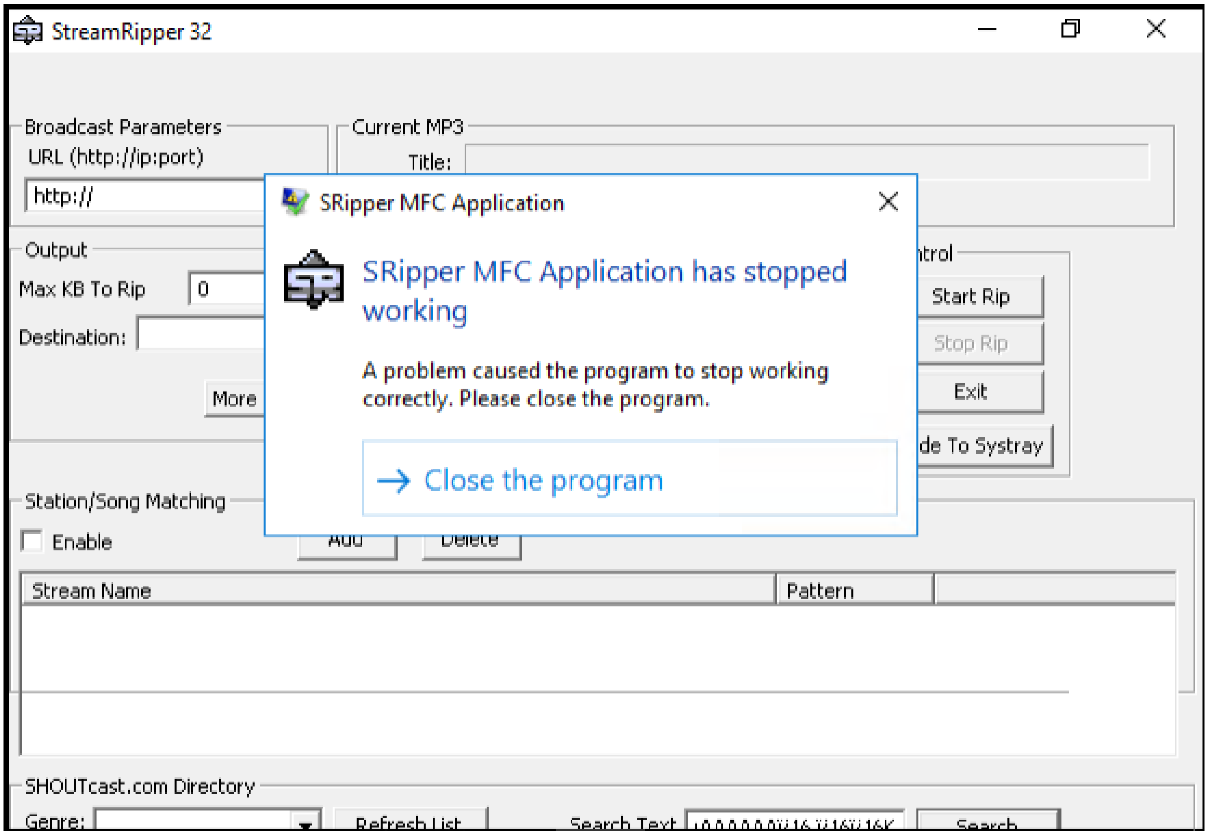
| | |
|---|---|
| **REMEDIATION** | • Addressing buffer overflow vulnerability.<br>• Input sanitization.<br>• Input validation (we may use regular expressions for validation).<br>• Implementing ASLR, DEP, SEH. |

| | |
|---|---|
| **References** | https://www.httpcs.com/en/php-shell-code-injection-vulnerability#:~:text=Shell%20Code%20Injection%20is%20an,system%20via%20a%20vulnerable%20application. |

## BUFFER OVERFLOW

| CVSS SEVERITY | High | | CVSSv3 SCORE | 8.9 |
|---|---|---|---|---|
| CVSSv3 CRITERIAS | Attack Vector : | **Network** | Scope : | **Changed** |
| | Attack Complexity : | **Low** | Confidentiality : | **High** |
| | Required Privileges : | **Low** | Integrity : | **Low** |
| | User Interaction : | **Required** | Availability : | **High** |
| AFFECTED SCOPE | | | | |
| DESCRIPTION | In a buffer overflow attack, the extra data includes instructions that are intended to trigger damaging activities such as corrupting files, changing data, sending private information across the internet, etc. An attacker would simply take advantage of any program which is waiting for certain user input and inject surplus data into the buffer. | | | |
| OBSERVATION | We have observed that buffer overflow potentially crash an application and unknowingly allows command injection attacks. | | | |

**TEST DETAILS**



SRipper MFC Application

SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Please close the program.

→ Close the program

Image 2 – image.png

| | |
|---|---|
| **REMEDIATION** | - ASLR<br>- DEP<br>- SEHOP |
| **REFERENCES** | www.cloudflare.com/learning/security/threats/buffer-overflow/ |

# DOM XSS

| | | | | |
|---|---|---|---|---|
| **CVSS Severity** | **High** | | **CVSSv3 Score** | **7.6** |
| **CVSSv3**<br>**Criterias** | Attack Vector : | **Network** | Scope : | **Changed** |
| | Attack Complexity : | **Low** | Confidentiality : | **High** |
| | Required Privileges : | **Low** | Integrity : | **Low** |
| | User Interaction : | **Required** | Availability : | **None** |
| **Affected Scope** | | | | |
| **Description** | **DOM XSS** stands for Document Object Model-based **Cross-site Scripting**. ... All HTML documents have an associated **DOM** that consists of objects, which represent document properties from the point of view of the browser. When a client-side script is executed, it can use the **DOM** of the HTML page where the script runs. | | | |
| **Observation** | `1)Open any url which you want to test let's say https://www.incrypts.com/`<br>` 2) now just put <html>` | | | |
| **Test Details** | | | | |
| **Remediation** | USE USER INPUT VALIDATION AND WAF | | | |
| **References** | | | | |