**Code Review Checklists of Croc Application**

Reviewer: Zexi Xing

Review Date: 12/02/2020

Code Size: 303 lines of code

File Name: utils.go

**Static Code Analysis**

|  |  |  |
| --- | --- | --- |
| Checklist Item | Category | Notes |
| Using CWE reference to analyze Croc’s structs and methods | Manual Code Analysis | If no automated Code Analysis is setup for Croc project, we do not use automatic analysis |

**Clean Code**

|  |  |
| --- | --- |
| Checklist Item | Category |
| Structs should be small | Structs |
| Functions should be small | Functions |
| Avoid duplication functions | Functions |
| Documentation properly | Comments |
| Do not return nil | Exceptions |
| Use intention-revealing names | Meaningful names |
| No spelling error | Meaningful names |
| File stream has been closed after used | Input Stream |

**Clean Performance**

|  |  |
| --- | --- |
| Checklist Item | Category |
| Avoid creating unnecessary process or threads | Creating and Destroying threads |

**Security Issues**

|  |  |  |  |
| --- | --- | --- | --- |
| Checklist Item | Weakness | CWE number | Category |
| Has not check the input string size before outputting it. | Improper Input Validation | CWE-20 | Input validation |
| Has not use check(err) method to check the input file size, also has not provide the malicious files validating algorithm | Unrestricted Upload of File with Dangerous Type | CWE-434 | Input validation |
| IsLocalIP() method always expose network configuration of Croc. | Exposure of Sensitive Information to an Unauthorized Actor | CWE-200 | Confidential information |
| Several hard-coded IP addresses always grant access to Croc file transferring and no other authentication is needed. | Improper Authentication  &  Use of Hard-coded Credentials  &  Reliance on IP Address for Authentication | CWE-287  &  CWE-798  &  CWE-291 | Confidential information |
| All valid IP credentials are viewable inside of a method | Insufficiently Protected Credentials | CWE-522 | Confidential information |
| All user will have the same privileges because Croc does not assign, modify, check privileges for an actor | Improper Privilege Management | CWE-269 | Access control |
| As long as the IP address is correct, Croc will not verify the user identity. | Missing Authorization | CWE-862 | Access control |
| Croc uses os.Open() to open the file and it is unsafe function. Hence, os.OpenFile() is a better choice. | Use of Potentially Dangerous Function | CWE-676 | Functions |
| Only checked if the slice is nil, and empty slice has never been validated | Incorrect Check of Function Return Value | CWE-253 | Functions |
| Uncontrolled for loop which designed for finding the missing chunks of file is recursively calling an append () function. | Uncontrolled Recursion  &  Excessive Iteration | CWE-834  &  CWE-674 | Functions |