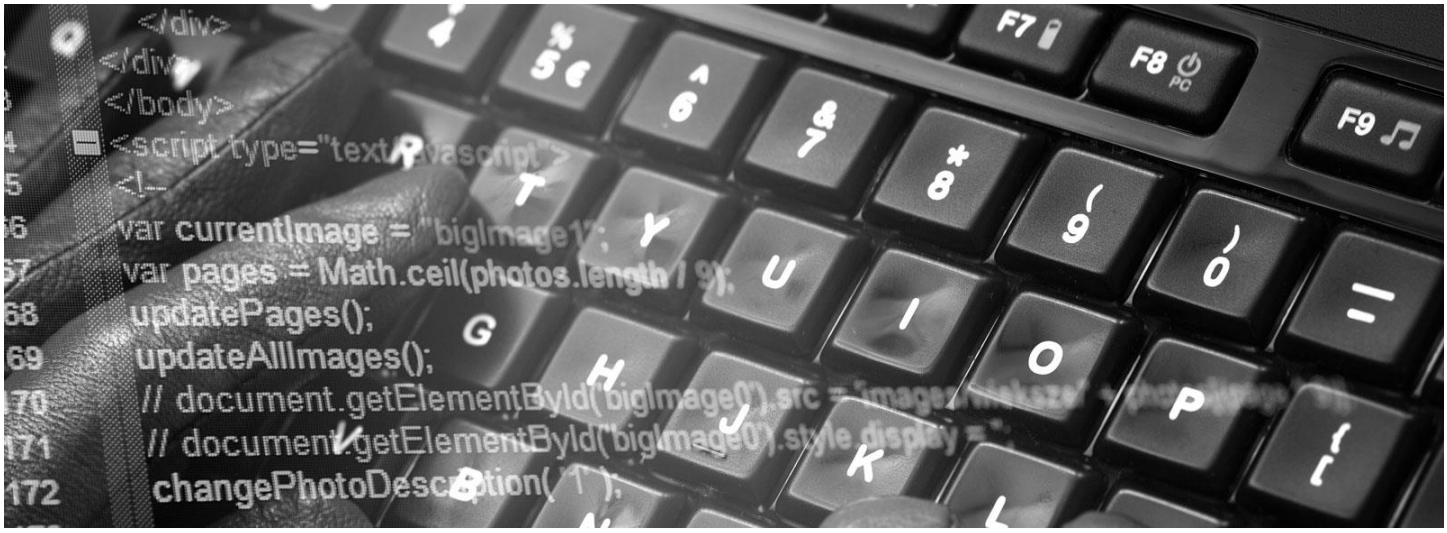
ISSUED ON: JULY 29, 2016

UL CYBERSECURITY ASSURANCE PROGRAM

Community of Trust RCoteCSIPIMcsBv1.2So09162015UL



PREPARED FOR:

Community of Trust Corporation
2020 K St. NW
Suite 1100 C/O Rob Bertin
Washington, DC 20006-1806

PREPARED BY:

MICHAEL JABLONSKI
JARED VOGEL
REVIEWED BY: KEN MODESTE
UL LLC, 333 Pfingsten Rd, Northbrook, IL 60062
PROJECT: 4787069208 REPORT NUMBER: 001

ALL RIGHTS RESERVED

DISCLAIMER

REPORT HISTORY

PRODUCT/SYSTEM VERSION:

Community of Trust Model RCoteCSIPIMcsBv1.2So09162015UL

REPORT REVISION HISTORY

Report Type	Date	Project Number
Pilot Program Evaluation	2016-03-09	4787069208
Review Updated Documentation	2016-04-20	4787069208
Review Update Documentation	2016-06-21	4787069208
Final Review Update Documentation	2016-07-06	4787069208
Final Review Update Documentation	2016-07-10	4787069208
Final Review Update Documentation	2016-07-28	4787069208

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Community of Trust version RCoteCSIPIMcsBv1.2So09162015UL was submitted to UL for an evaluation to the Standard for Software Cybersecurity for Network-Connectable Products, UL 2900-1, and Edition Number: 1 dated March 30 2016.

This product was found to be in compliance with the Standard and Certificate ULCAP_100 issued on July 29th 2016 was issued to Community of Trust Corporation for this product.

PRODUCT DESCRIPTION

The Community of Trust Model RCoteCSIPIMcsBv1.2So09162015UL, Technological Solution (CoT) utilizes a multi-layered encryption software approach. This creates a secure encrypted connection while cloaking the IP accessibility of the edge devices connected to a Community of Trust. Traffic from all the edge devices inside the Community of Trust is policed and anomalous or suspicious traffic is captured and stored in the Central Privacy Authority Intrusion Database, which is a key component of the functionality of a Community of Trust.

CRITICAL HARDWARE COMPONENTS

Table 1 below lists the hardware components that were evaluated as part of the RCoteCSIPIMcsBv1.2So09162015UL system:

Hardware			
Component	**Function**	**Manufacturer**	**Model/Version**
NUC5i7RYH Small Form Factor CPU	Server	Intel	UPC 735858297066
WRT1200AC	Router	Linksys	EA6100

Table 1

CRITICAL SOFTWARE COMPONENTS

Table 2 below lists the software components that were evaluated as part of the RCoteCSIPIMcsBv1.2So09162015UL system:

Software			
Component ID	**Notes**	**Manufacturer**	**Model/Version**
RHEL Server 6.7 x86_64	Operating System	Red Hat	6.7
Kamailio	SIP Server V 4.3.1. Used under GPL V2	Open Source	4.3.1
OpenSSL	Cryptographic Library	Open Source	1.0.1e-42.e16 FIPS 11 February 13
FIPS Cryptography	Under Apache License 1.0	Apache	2.0.6
StrongSwan	Open Source IPSec for Linux, ISO 19770-2 regid 2004-03 Version U5.3.2/K2.6.32-573.8.1.el6.x86_64	Open Source	5.3.2
Ejabberd	XMPP Application Server	Open Source	15.07.33
GMP	Precision Arithmetic Library Used under GNU LGPL V3 and GNU GPL V2	Open Source	4.3.1-7.el6_2.2
Flex	(The Fast Lexical Analyzer) Lexical Analysis Used under the BSD license	Open Source	2.5.35-9.el6.x86_64
Bison	A GNU general purpose parser used by Kamailio for parsing the SIP strings.Used under GPLV3+	Open Source	2.4.1-5.el6.x86_64

Erlang	V.18.0 A general purpose programming language optimized for concurrent programming	Open Source	V.18.0 A
MySql	General purpose SQL Database. V. 5.1.73 from RedHat Repository	Red Hat	5.1.73
RTPproxy	General purpose utility (/usr/local/bin) supporting VoIP traffic thru firewalls using the Real-time Transport Protocol	Open Source	20040107
SKS Keyserver	OpenPGP Keyserver for the OpenPGP Encryption	RedHat	sks-1.1.5-9.el6.x86_64

Table 2

CRITICAL DOCUMENTATION COMPONENTS

Table 3 below lists the critical documentation components that were evaluated as part of the RCoteCSIPIMcsBv1.2So09162015UL system:

Documentation	
Name	**Version**
Detailed Component Specifications	RcoteCSIPIMcsBv1.2So09162015UL_Bill_Of_Materials- June 2016 v.1.02
Risk Profiles and Attack Vectors -An Assessment of the Risk Exposures in the Community of Trust Architecture	June 2016 v. 1.02
Detailed Component Specifications	RcoteCSIPIMcsBv1.2So09162015UL -March 2016 v. 1.0 Supplement Software Listing

Table 3

Table 4 contains accompanying hardware and software used during testing of the product. These components were used in evaluation of the product BUT ARE NOT part of the certification and WAS NOT ASSESSED.

Accessory Components Used During Testing			
Component	**Function**	**Manufacturer**	**Model/Version**
LG Android Tablet	Messaging Client to the Product	LG	Model LG-V480, Android version 5.02, Kernel version

			3.4.0+, Software version V48020b
LG Android Tablet	Messaging Client to the Product	LG	Model LG-V400, Android version 5.02, Kernel version 3.4.0+, Software version V40020a

Table 4

CUSTOMER'S CONFIRMED INTENDED USE/ CONFIGURATIONS

The product's intended use is described in its user documentation. The product was evaluated with the following configurations and is intended to be operated as such:

1. All communication is restricted to inside the Encrypted Core VPN, and except for the ports specifically addressing the VPN structure, all TCP ports are closed to external access. Mandatory open ports include Ipsec-nat-t (TCP/UDP Protocol/Port 4500, RFC 3947) and ISAKMP (TCP/UDP Port/Protocol 500) and a port range for RTPproxy nat transversal (UDP Protocol range 20,000-30,000). All other ports are blocked and remote access outside the VPN is not permitted.
2. Remote access via SSH or Remote Desktop is never permitted, and Root login via SSH is not permitted under any circumstances.
3. An external facing router shall be configured to the manufacturer's specifications to restrict port access listed in item 1 of this section.

CONDITIONS OF CERTIFICATE

See certificate for conditions of certificate.
The following conditions must be met for the product to continue to be in compliance with this certificate:

1. An external router shall be configured to requirements specified in the user documentation. Supporting software & hardware, router with the configuration and firewall settings located in the documentation Detailed Component Specifications RcoteCSIPIMcsBv1.2So09162015UL dated June 2016 v.1.02RcoteCSIPIMcsBv1.2So09162015UL in section 4.6.8 Router Configuration and 4.6.9 Router Configuration Template.
2. The following version of software included in the product is applicable:
    a. Red Hat Enterprise Security Enhanced Linux RHEL Server 6.7 x86_64-6.7
    b. Kamailio-SIP Server V 4.3.1. Used under GPL V2
    c. OpenSSL-Version 1.0.1e-FIPS 11
    d. FIPS CryptographyV. 2.0.6
    e. StrongSwanVersion 5.3.2
    f. Ejabberd XMPP Application Server. V. 15.07.33
    g. GMP Used under GNU LGPL V3 and GNU GPL V2 - 4.3.1-7.el6_2.2
    h. Flex v2.5.35-9.el6.x86_64

i. Bison v 2.4.1-5.el6.x86_64
j. Erlang V.18.0 A
k. MySql V. 5.1.73
l. RTPproxy Github basic version 20040107 dated 9/11/2015
m. SKS KeyserverOpenPGP Keyserver v sks-1.1.5-9.el6.x86_64

3. There is no connectivity; for example WiFi, LTE or Ethernet except via the VPN.
4. The product certification does NOT support IKEv1.
5. This certification does not cover the client software (tablets, phone, external messaging devices) .

SCOPE OF EVALUATION

The product evaluated was limited to all criteria as defined in the UL 2900-1 standard. The scope of the evaluation required the setup of the product on an Intel next unit of computing (NUC) with an Apple iPad and LG Tablet used for communications. The NUC was protected by an external LinkedSys router. The product utilizes a multi-layered encryption mechanism that creates a secure encrypted connection while cloaking the IP accessibility of the edge devices connected to a Community of Trust. Traffic from all the edge devices inside the Community of Trust is policed and anomalous or suspicious traffic is captured and stored in the Central Privacy Authority Intrusion Database, which is a key component of the functionality of a Community of Trust. The product was assessed for the following:

1. Scanning for known malware on the product binaries.
2. Scanning for known vulnerabilities reported in the NIST National Vulnerability Database (NVD).
3. Scanning for common software weaknesses in the source code and binaries of the product as defined in the UL 2900-1 standard.
4. Subjecting the product to malformed traffic data on the protocols and interfaces identified in the product that are accessible to an outside party.
5. Evaluation and assessment of the product per security controls defined in the UL 2900-1 standard such as access control and authentication, remote connections, software integrity, cryptography, security logs and decommissioning of the product.
6. Evaluation of Community of Trust risk assessment based on discovered issues per the UL 2900-1 standard.
7. Structured penetration testing based on Community of Trust final risk assessment to identify any issues that may be uncovered based on the risk assessment and the following parameters of the UL 2900-1 standard:
   a) Circumvent the risk controls and security configuration of the product;
   b) Attempt to engage the product in a denial of service;
   c) Attempt to access and authenticate on the product via unauthorized means;
   d) Attempt to exploit vulnerabilities acceptable in the risk analysis;
   e) Attempt to elevate privilege on the product.
   f) Attempt a man in the middle attack on the product.

CERTIFICATION

The certificate if valid, can be located at UL's Online Certification Database as ULCAP_100.

The certificate is still valid if the product continues to comply with the standard, the evaluation described in this summary report is still accurate, the product remains unchanged and no other vulnerabilities have been discovered and reported to the NIST National Vulnerability Database.

SUMMARY OF RESULTS

The product was found to be compliant with the Standard for Software Cybersecurity for Network-Connectable Products, UL 2900-1, and Edition Number: 1 dated March 30th 2016.

The below section defines a summary of the results of testing. All test records and test reports are recorded within the UL data system with details on actual tests, tool versions and full test results.

KNOWN VULNERABILITY TESTING SUMMARY

The product was scanned with the following tools to assess any known vulnerabilities that may exist in the product that is reported in the NIST National Vulnerability Database.

Table 5 below lists the tools that were used to evaluate the RCoteCSIPIMcsBv1.2So09162015UL system for known vulnerabilities per section 13; Known Vulnerability Testing of the UL 2900-1 standard.

Known Vulnerability Testing		
Component	**Date Tested**	**Tool Used**
Erlang and Flex	2015-09-30	Synopsys Protecode
Full Product	2016-01-30	Synopsys Protecode
All Critical Components in Table 2	2016-02-10	Synopsys Protecode
Full Product	2016-03-08	Rapid 7 Metasploit Pro
Erlang and Flex	2016-03-29	Synopsys Protecode
All Critical Components in Table 2	2016-03-29	Synopsys Protecode
All Critical Components in Table 2	2016-06-27	Synopsys Protecode
All Critical Components in Table 2	2016-07-21	Synopsys Protecode

Table 5

There was a total of 1296 CVEs found in our assessment in 33 components of the product with the largest quantities found in the following:

1. Linux kernel – 713 CVEs identified
2. PHP – 236 CVEs identified
3. OpenSSL – 92 CVEs identified
4. GLIBC – 87 CVEs identified

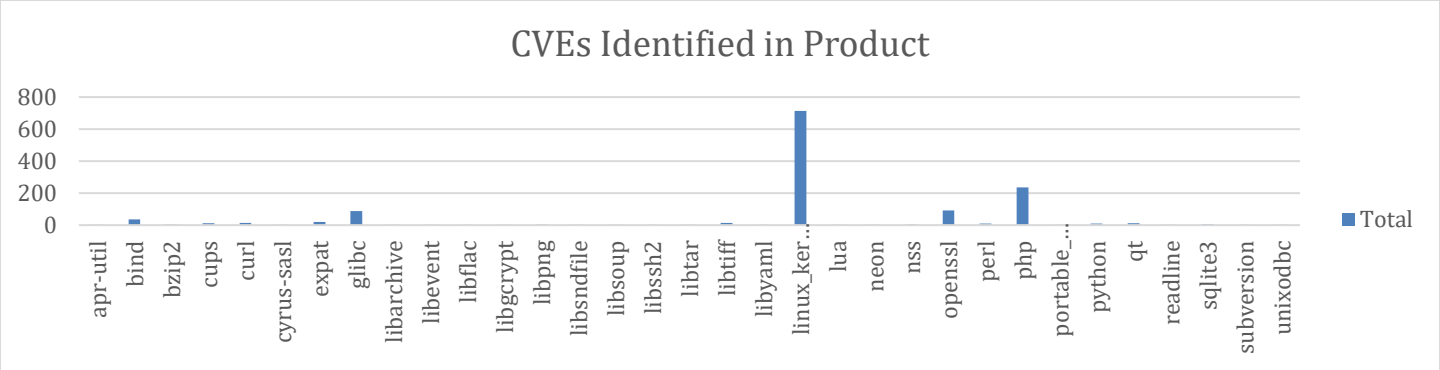


Chart 1

The risk assessment performed by the client provided the following results in Chart 2:

1. Closed – Items resolved in the current release with the Red Hat Security Advisory (RHSA) noted. Closed items do not affect the current installation.
2. Low Impact - Numerous vulnerabilities categorized as low impact, will not fix are of insignificant impact, usually require root privileges to execute, and are fully mitigated by in the risk assessment file.
3. Not Applicable - Not Applicable items typically address functions or protocols either not supported by Red Hat at all, or not supported in the current installation. e.g. PHP is NOT a part of the supported software while present ad the interface is not exposed to the client.
4. Rejected – Rejected items were rejected by the Red Hat Security Team as not being a valid security concern and thus are not legitimate issues.
5. Active - Active security concerns designate significant flaws in the affected software for which there is no available patch or resolution. There are at present ZERO active security concerns listed.

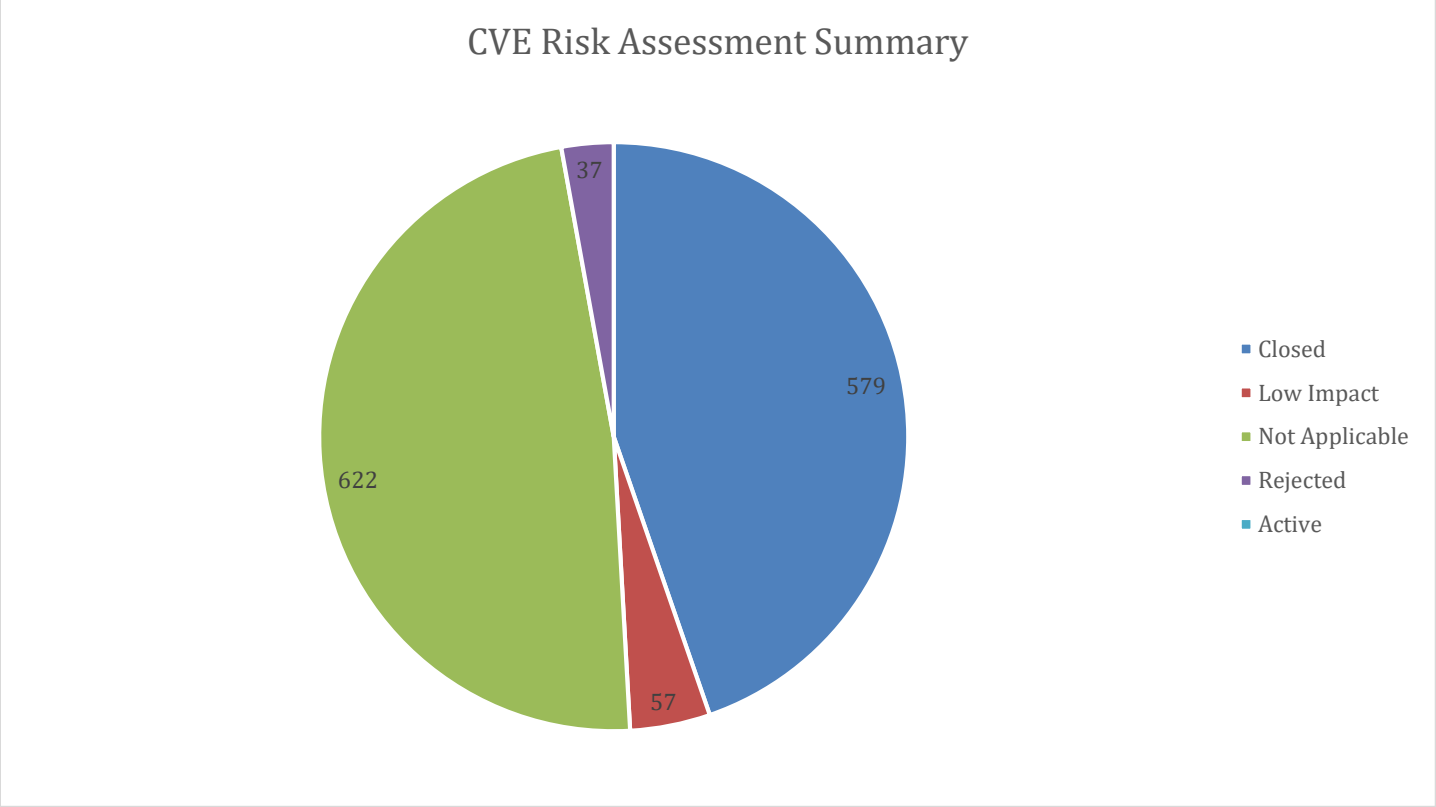


Chart 2

Chart 3 provides a summary of the risk assessment done on the CVEs per components in the product. UL evaluated the risk assessment and we validated the following:

1. Items marked as closed were identified as not relevant as part of the product's current configuration.
2. Items marked as not applicable were identified as not relevant as part of the product's current configuration.
3. Items marked as rejected by the Red Hat Security Team was evaluated and assessed as not part of the product's current configuration.
4. All CVEs were attempted to exploit in the existing configuration. Because the product uses an encrypted core with an IPSEC tunneling capability with limited ports open, UL LLC was unable to exploit the CVEs identified. UL used the Rapid7 Metasploit Pro existing CVE exploits to attempt to exploit the Not applicable and low impact CVEs.
5. There were no active CVEs that were exploitable that UL LLC was able to identify.
6. The last date the vulnerability scan was executed was on **July 21st 2016**. One additional CVE CVE-2016-2775 was found in the Bind Version bind-9.8.2-0.37.rc1.el6_7.6.x86_64 that is included in product.
    a. Date 2016-07-19 – CVSS v2 Base Score: 4.3 – Exact match
    b. ISC BIND 9.x before 9.9.9-P2, 9.10.x before 9.10.4-P2, and 9.11.x before 9.11.0b2, when lwresd or the named lwres option is enabled, allows remote attackers to cause a denial of service (daemon crash) via a long request that uses the lightweight resolver protocol.
    c. This is not an issue in this system because lwresd or the named lwres are not being used therefore are not enabled.
    d. This vulnerability is **NOT APPLICABLE** to the product.

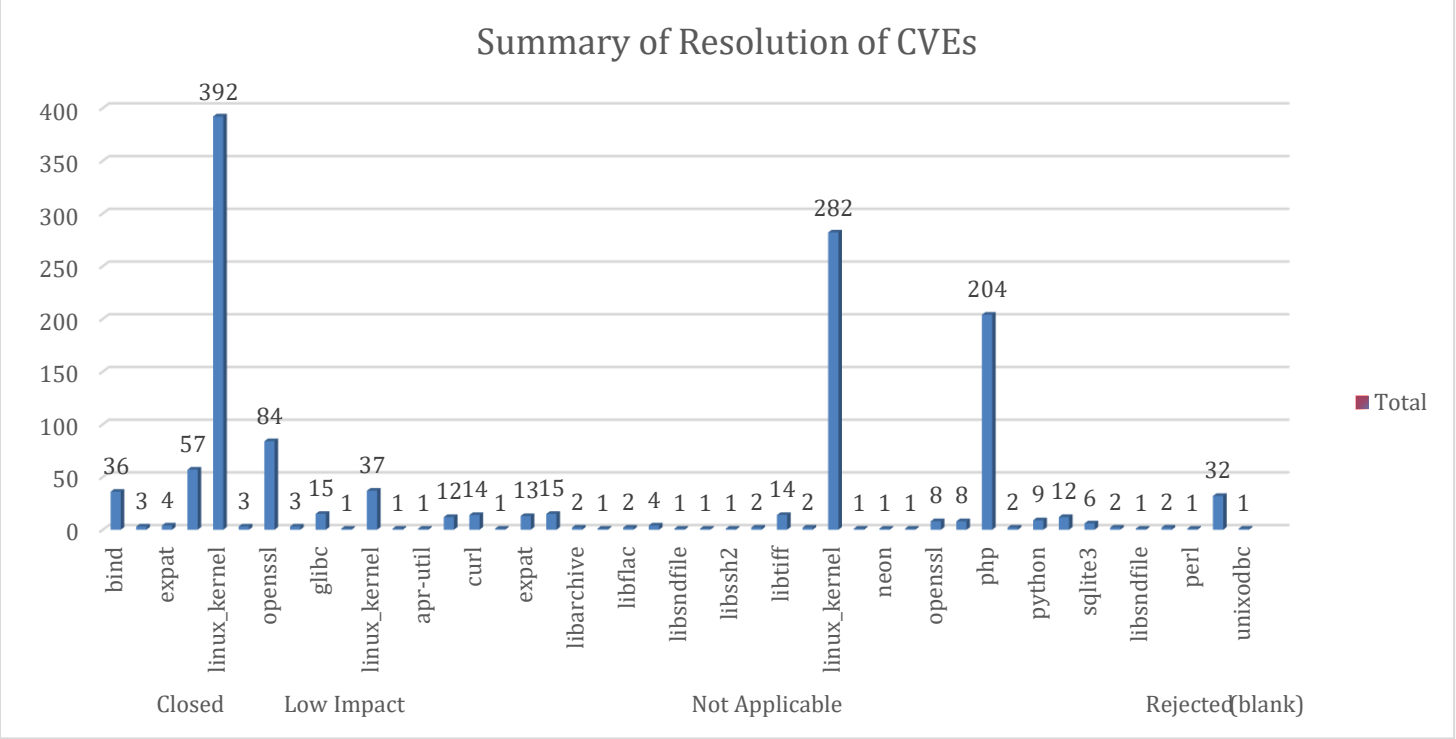


Chart 3

MALFORMED INPUT TESTING SUMMARY

The product was subjected to Malformed Input Testing (Fuzz Testing) per section 15 of UL 2900-1. The tests that were performed attempted to exercise weaknesses in the TLS capability around the following areas:

1. Numeric Errors
2. Data handling of messages
3. Wrap around errors
4. Improper validation of Array Index
5. Integer overflows
6. Signed to unsigned conversion errors
7. Incorrect numeric conversions
8. Numeric range Validations
9. Buffer overflows
10. Improper handling of invalid data in messages

Table 6 below lists the tools that were used to evaluate the RCoteCSIPIMcsBv1.2So09162015UL system for malformed input testing per section 15 of the UL 2900-1 standard and a summary of the results

Malformed Input Testing			
Test Description	**Date Tested**	**Tool**	**Results**
TCP for IPV4 Test Cases	2016-03-09	Synopsys Defensics v11.10.12 for Windows	The product went into denial of service but recovered after 13 seconds
TCP for IPV4 Test Cases	2016-03-10	Synopsys Defensics v11.10.12 for Windows	The product went into denial of service but recovered after 13 seconds
ICMPv4	2016-03-10	Synopsys Defensics v11.10.12 for Windows	The product went into denial of service but recovered after 13 seconds
IPSec Test Cases	2016-03-10	Synopsys Defensics v11.10.12 for Windows	The tests were unable to complete as the product continued to deny access to the communication channel
ISAKMP Test Cases	2016-03-23	Synopsys Defensics v11.10.12 for Windows	The tests were unable to complete as the product continued to deny access to the communication channel
TLS Server Test Cases	2016-03-23	Synopsys Defensics v11.10.12 for Windows	Executed all test cases and passed without event
ARP Server Test Cases	2016-03-28	Synopsys Defensics v11.10.12 for Windows	Executed all test cases and passed without event

Table 6

The product testing on 2 tests were unable to complete as the product continued to deny access to the communication channel to continue fuzzing. The connection was denied as per the setup of the product. The product is expected to continue to deny attempts on invalid access through its encrypted tunnel. The product did go into a denial of service but was able to recover in 13 seconds to continue to receive valid instructions and data.

MALWARE TESTING

All software binaries listed by the vendor according to UL 2900-1 Section 14 was evaluated for known malware. This included all executables and libraries in the product, including all third party and open source software. The product was scanned with Sophos SAVScan virus detection utility Version 5.21.0, Virus data version 5.22, December 2015
Includes detection for 10433658 viruses, Trojans and worms (Copyright (c) 1989-2015 Sophos Limited.)

50864 files were scanned.
14 errors were encountered.
No viruses were discovered.

Files that could not be found by SAVScan were reviewed manually. The 14 errors identified are Orphaned Symbolic links and are not assessed as Malware.
The software binaries under test DO NOT contain known malware at the time of evaluation.

CODE, BINARY AND BYTE CODE ANALYSIS SUMMARY

Table 7 captures the following critical components of the product that were assessed using the Synopsys Coverity Static Analysis Tool v 7.7.0.

Software Weakness Testing		
Component	**Date Tested**	**Tool Used**
StrongSwan Linux Version U5.3.2/K2.6.32-573.8.1.el6.x86_64	2016-01-28	Coverity v 7.7.0
OpenSSL Version 1.01e-fips 11 Feb 2013	2016-02-03	Coverity v 7.7.0
RTP Proxy Version	2016-02-11	Coverity v 7.7.0
Kamailio Version SIP Server V 4.3.1	2016-02-11	Coverity v 7.7.0

Table 7

The analysis found 927 weaknesses by the tool. The customer provided a risk assessment of all 927 software weaknesses. These weaknesses found by the tool was both a combination of security issues, quality issues, programming standard issues and the OWASP Top 10 and SANS Top 41 software security weaknesses.

These can be found in Chart 4 below:

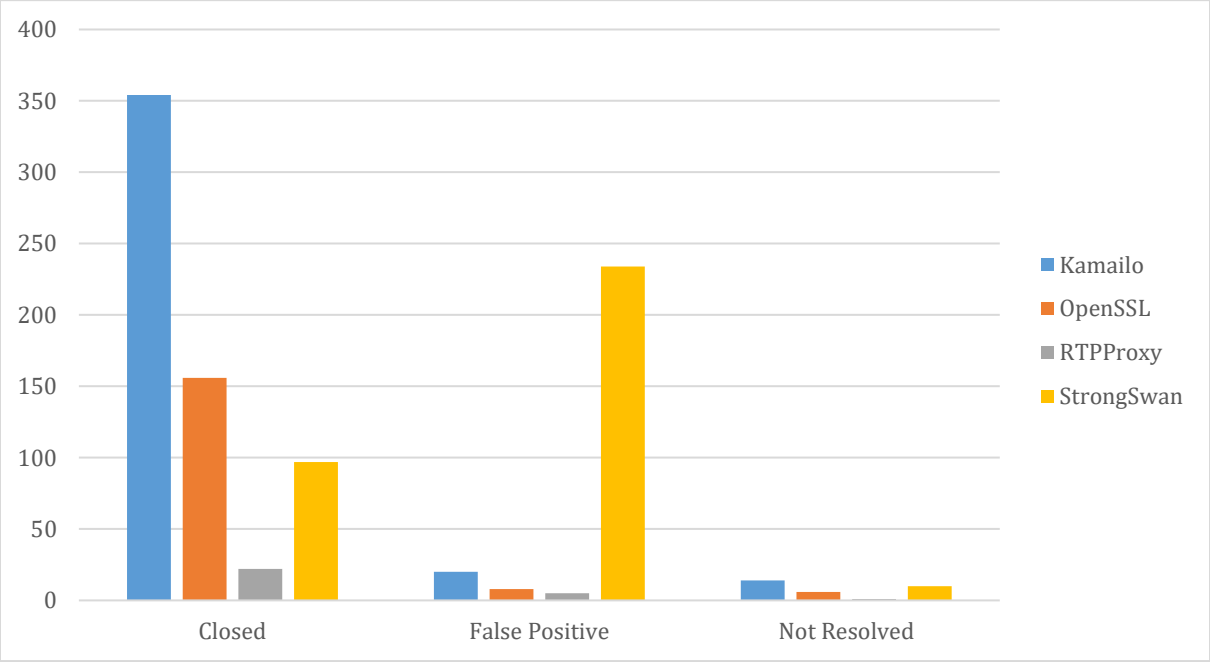


Chart 4

UL LLC assessed only the weaknesses found that were in the OWASP Top 10 and the SANS Top 41 per UL 2900-1 standard. These can be found in Chart 5 below.

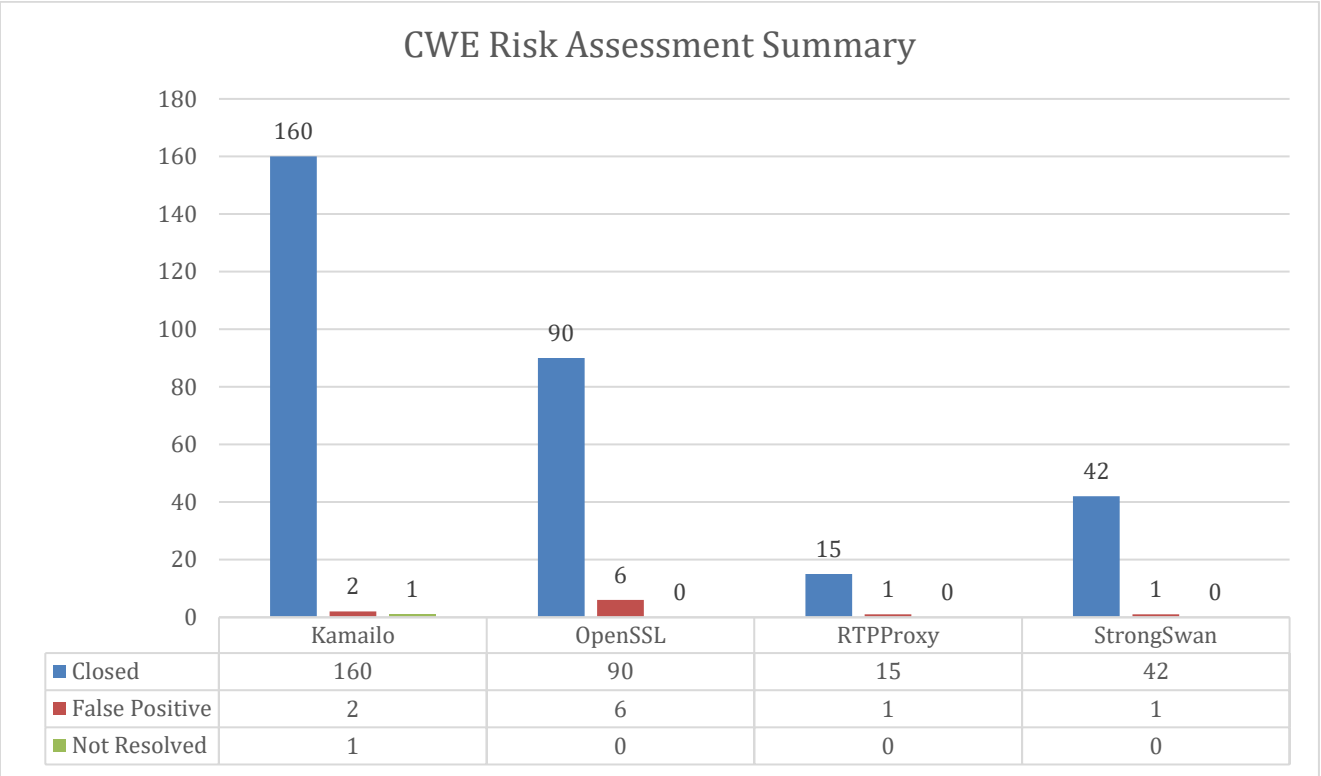


Chart 5

The following assessments were observed based on the software weakness analysis and the customer's response in the risk assessment file. They can be found in Table 8

Software Weakness Testing		
OWASP Top 10		
Clause # Ranking	Finding	Resolution
N/A	No OWASP Top 10 software weaknesses were identified in the components assessed.	This provided compliance to the requirements of UL 2900-1 Section 17 and Appendix A1 Sources for Software Weaknesses OWASP Top 10
SANS Top 41		
KAMAILO COMPONENT – See Charts 4,5,6		
Clause # Ranking	Finding	Resolution
CWE-190 #24	INTEGER OVERFLOW OR WRAPAROUND 2 Found. An inferred misuse of an enum where a potential integer overflow could occur in a parser. Vendor identified to not resolve issue. Discovered in a read of a reply message where an index to be read may be truncated based on the type of the variable.	UL LLC's assessment of this weakness determined that a parameter passed to a parser reading the input to the SIP server was correct based on the values being passed and the error checking occurring in the module. This CWE is considered a false positive. Both the vendor and UL's assessment determined that the read from a TCP or UDP port using a possible truncated value is a false positive. The value to be read is always smaller than the variable being used and truncation should not be an issue.

CWE-676 #18	USE OF POTENTIALLY DANGEROUS FUNCTION) 28 Found Use of a weak random number generator i.e random, rand. The Vendor risk assessment describes that rand() provides random numbers with entropy satisfactory for FIPS 140-2 cryptography under RH SELINUX using the hwrng device. It is acceptable	These are in the communication sections of kamailo which are encapsulated by the use of the VPN tunnel generated by OpenSSL. These CWEs are considered not an issue. Also rand() has been acceptable for entropy once the seed is generated by hwrng.
CWE-120 #3	BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') 16 Found Use of a fixed length string without checking the length.	The major component in Kamailo affected by this CWE was in assigning IP addresses in the underlying RTPproxy module. The IP addresses are entered into the system directly per the configuration setup and the ability for malicious intent to modify is not considered an issue.
CWE-394 #28	IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS 3 Found The TCP connection is passed to an unsigned variable.	This should not cause a problem since ids after creating a TCP connection are in signed numbers, but was evaluated in the penetration testing section while testing the TCP connection and in malformed input testing.
CWE-252 #28	UNCHECKED RETURN VALUE 50 found In many modules of Kamailo where a function's return value was not checked for error validation. Vendor risk assessment states that not checking return value is bad form, but not strictly necessary in many instances.	This CWE is not ranked in the top 41 but is related to #28 of improper checking for error conditions. An unexpected return value could place the system in a state that could lead to a crash or other unintended behaviors however this particular CWE is not covered under UL 2900-1. Penetration testing around exception handling was performed.
CWE-476 #36	NULL POINTER DEREFERENCE 54 Found. Discovered in Kamailo's modules for DNS caching, RTPProxy, address lookup and library files. The vendor risk assessment described these CWEs as closed as they determined the found weaknesses may have not followed proper coding standard practices, they did not represent a significant risk with limited security potential errors.	Many of the null pointer dereference issues were tested as part of the section on penetration testing of the Kamailo SIP server.
CWE-129 #27	IMPROPER VALIDATION OF ARRAY INDEX 2 Found Discovered in the reading of SIP messages once communications has been established. Vendor risk assessment has determined these items are not an issue	These 2 issues in the source code are associated with using array indices without validation of the size and sign. UL LLC has determined that the types of the variables have a potential for being signed negative which may cause memory access problems, however, review of the surrounding code determined this is a false positive result as the likelihood is negligible. Penetration testing and malformed input testing addresses these potential issues

CWE-367 #33	CONCURRENT EXECUTION USING SHARED RESOURCE WITH IMPROPER SYNCHRONIZATION ('RACE CONDITION') 8 Found Discovered in several modules of Kamailo that are checking. The vendor risk assessment has determined some are not an issue and closed and some are false positive	Checking if a file exists before opening it is a good practice. It is poor security practice to not lock the file prior to checking, then using the file, then unlocking it. Such synchronization is important, however does not impact the security hygiene in this product
SANS Top 41		
OPENSSL COMPONENT – See Charts 4,5,7		
Clause # Ranking	Finding	Resolution
CWE-120 #3	BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') 1 Found Discovered setting a string value into a 256 byte size string without checking string value.	The string values are predefined error messages that fall below the 256 byte size. The CWE cannot occur. This is considered a false positive.
CWE-190 #24	INTEGER OVERFLOW OR WRAPAROUND 1 Found. Discovered in the random number generator of the crypto module, where a calculated value is used as an argument for a function without checking if the value meets the parameter type.	The calculated value meets the parameter of the function. This is considered a false positive.
CWE-252 #28	UNCHECKED RETURN VALUE 38 found In many modules of Kamailo where a function's return value was not checked for error validation. Vendor risk assessment states that not checking return value is bad form, but not strictly necessary in many instances.	This CWE is not ranked in the top 41 but is related to #28 of improper checking for error conditions. An unexpected return value could place the system in a state that could lead to a crash or other unintended behaviors however this particular CWE is not covered under UL 2900-1. Penetration testing around exception handling was performed.
CWE-367 #33	CONCURRENT EXECUTION USING SHARED RESOURCE WITH IMPROPER SYNCHRONIZATION ('RACE CONDITION') 2 Found Discovered in random number generator of the crypto module. The vendor risk assessment has determined some are not an issue and closed and some are false positive.	Checking if a file exists before opening it is a good practice. It is poor security practice to not lock the file prior to checking, then using the file, then unlocking it. Such synchronization is important, however does not impact the security hygiene in this product significantly.
CWE-197 #35	NUMERIC TRUNCATION ERROR 1 Found Discovered in the crypto module where a signed number is cast into an unsigned long	This CWE is not ranked in the top 41 but is related to #35 of improper number conversion. Typically, when a primitive is cast to a smaller primitive, the true value can be lost and corrupted data can be used instead. However this particular CWE is not covered under UL 2900-1.
CWE-476 #36	NULL POINTER DEREFERENCE 54 Found. Discovered in OpenSSL multiple. The vendor risk assessment described these CWEs as	Extensive penetration testing of the OpenSSL communications did not identify any issue.

	closed as they determined the found weaknesses may have not followed proper coding standard practices, they did not represent a significant risk with limited security potential errors.	
SANS Top 41		
RTPPROXY COMPONENT – See Charts 4,5,8		
Clause # Ranking	Finding	Resolution
CWE-120 #3	BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') 2 Found Discovered setting a string value into sprintf or a fixed size string	The string values are predefined messages that fall below the 256 byte size and the length is set prior to use. The CWE cannot occur. This is considered a false positive.
CWE-676 #18	USE OF POTENTIALLY DANGEROUS FUNCTION) 28 Found Use of a weak random number generator i.e rand. The Vendor risk assessment describes that rand() provides random numbers with entropy satisfactory for FIPS 140-2 cryptography under RH SELINUX using the hwrng device. It is acceptable	These are in the main section of RTPProxy which are encapsulated by the use of the VPN tunnel generated by OpenSSL. These CWEs are considered not an issue. Also rand() has been acceptable for entropy once the seed is generated by hwrng.
CWE-190 #24	INTEGER OVERFLOW OR WRAPAROUND 1 Found. Discovered in the rtpserver, where a return value is cast into a larger numeric type	The return value doesn't lose or wraparound its value.
CWE-129 #27	IMPROPER VALIDATION OF ARRAY INDEX 1 Found Use of an array index without checking variable	Validated that the variable is set prior to use that is within the bounds of the array.
CWE-252 #28	UNCHECKED RETURN VALUE 7 Found In the main module of RTPProxy where a function's return value was not checked for error validation. Vendor risk assessment states that not checking return value is bad form, but not strictly necessary in many instances.	This CWE is not ranked in the top 41 but is related to #28 of improper checking for error conditions. An unexpected return value could place the system in a state that could lead to a crash or other unintended behaviors however this particular CWE is not covered under UL 2900-1. Penetration testing around exception handling was performed.
CWE-476 #36	NULL POINTER DEREFERENCE 2 Found. The vendor risk assessment described these CWEs as closed as they determined the found weaknesses may have not followed proper coding standard practices, they did not represent a significant risk with limited security potential errors.	Extensive penetration testing of the RTPProxy communications did not identify any issue.
SANS Top 41		
STRONGSWAN COMPONENT – See Charts 4,5,9		
Clause	Finding	Resolution

# Ranking		
CWE-676 #18	USE OF POTENTIALLY DANGEROUS FUNCTION) 11 Found Use of a weak random number generator i.e rand. The Vendor risk assessment describes that rand() provides random numbers with entropy satisfactory for FIPS 140-2 cryptography under RH SELINUX using the hwrng device. It is acceptable	These are in the multiple sections of StrongSwan which are encapsulated by the use of the VPN tunnel generated by OpenSSL. These CWEs are considered not an issue. Also rand() has been acceptable for entropy once the seed is generated by hwrng.
CWE-129 #27	IMPROPER VALIDATION OF ARRAY INDEX 1 Found Use of a variable without validating it is >=0	Validated that the scenario of the variable <0 does not occur
CWE-252 #28	UNCHECKED RETURN VALUE 7 Found fread function's return value was not checked for error validation. Vendor risk assessment states that not checking return value is bad form, but not strictly necessary in many instances. The source code actually does validate fread's value – FALSE POSITIVE	This CWE is not ranked in the top 41 but is related to #28 of improper checking for error conditions. An unexpected return value could place the system in a state that could lead to a crash or other unintended behaviors however this particular CWE is not covered under UL 2900-1. Penetration testing around exception handling was performed.
CWE-394 #28	IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS 2 Found A variable that can hold a negative value is passed to an unsigned variable	Validated that the variable is unlikely to have a negative value.
CWE-367 #33	CONCURRENT EXECUTION USING SHARED RESOURCE WITH IMPROPER SYNCHRONIZATION ('RACE CONDITION') 5 Found Found with using the stat() and access() function. The vendor risk assessment has determined some are not an issue and closed and some are false positive.	Checking if a file exists before opening it is a good practice. It is poor security practice to not lock the file prior to checking, then using the file, then unlocking it. Such synchronization is important, however does not impact the security hygiene in this product significantly.
CWE-476 #36	NULL POINTER DEREFERENCE 18 Found. The vendor risk assessment described these CWEs as closed as they determined the found weaknesses may have not followed proper coding standard practices, they did not represent a significant risk with limited security potential errors.	Extensive penetration testing of the StrongSwan communications did not identify any issue.
CWE-416 #40	USE AFTER FREE 4 Found. The vendor risk assessment described "There is no indication that it reads from the pointer after it is freed. It is set to NULL and the loop exited."	The dereferencing of the pointer identified by the tool cannot be validated. The pointers are all local and are dereferenced to zero on exit of the function, not prior. This CWE is not ranked in the top 41 but is related to #40 of expired pointer reference. This particular CWE is not covered under UL 2900-1.

Table 8

Chart 6 Below summarizes the SANS Top 25 and the SANS on the cusp (26-41) Common Weakness Enumerators found in the Kamailo component of the product

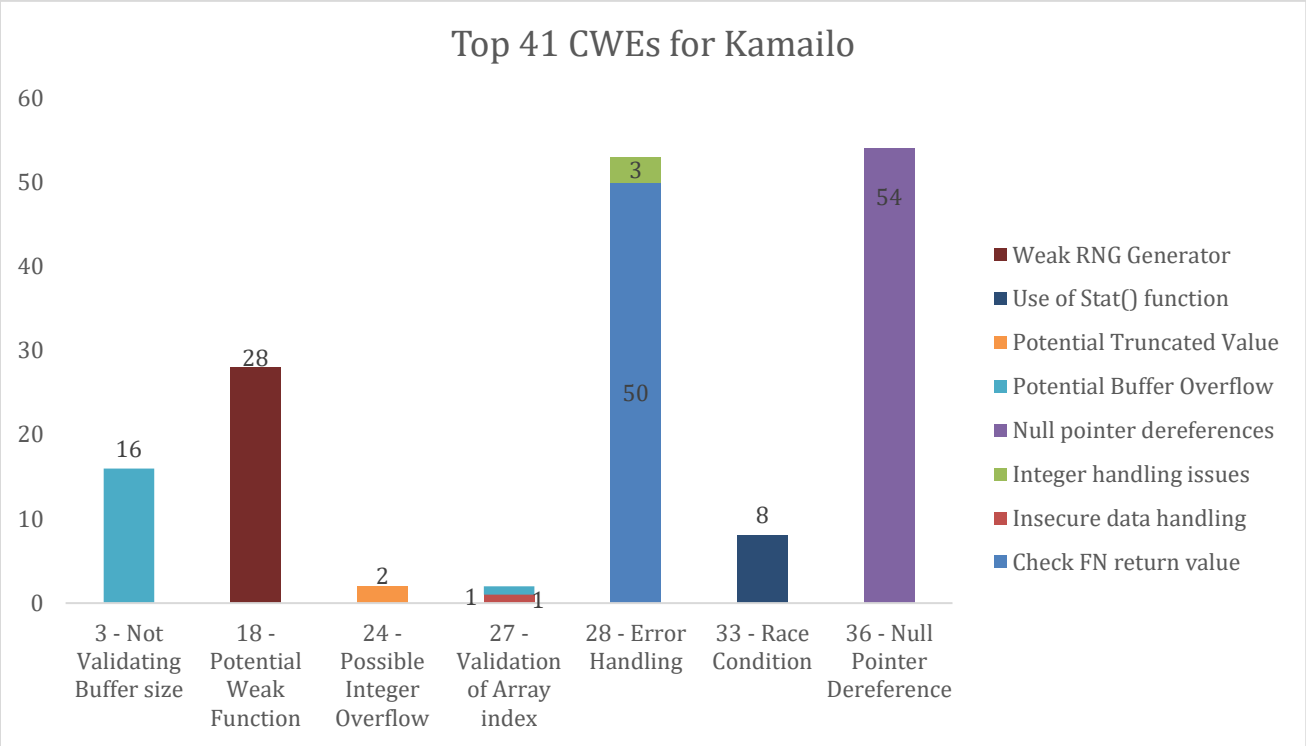


Chart 6

Chart 7 below summarizes the SANS Top 25 and the SANS on the cusp (26-41) Common Weakness Enumerators found in the OpenSSL component of the product.

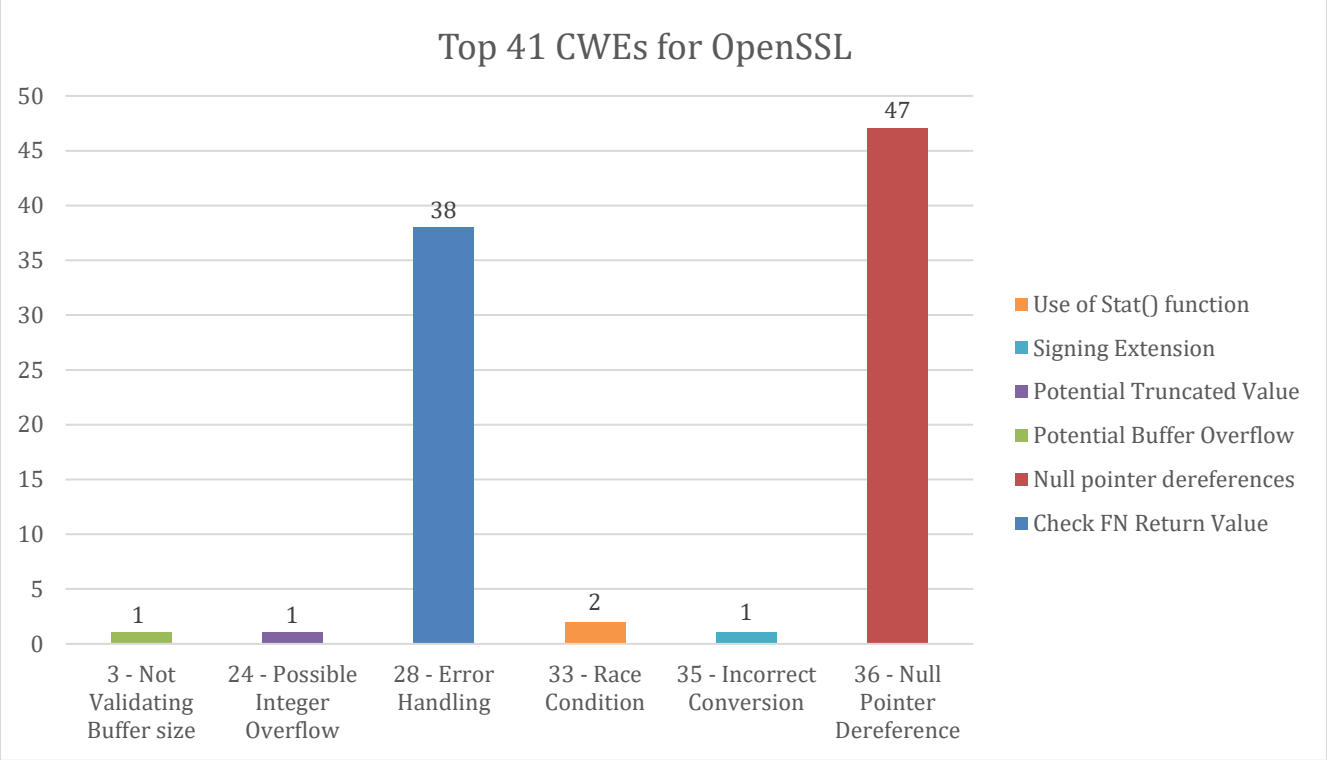


Chart 7

Chart 8 Below summarizes the SANS Top 25 and the SANS on the cusp (26-41) Common Weakness Enumerators found in the RTPProxy component of the product.

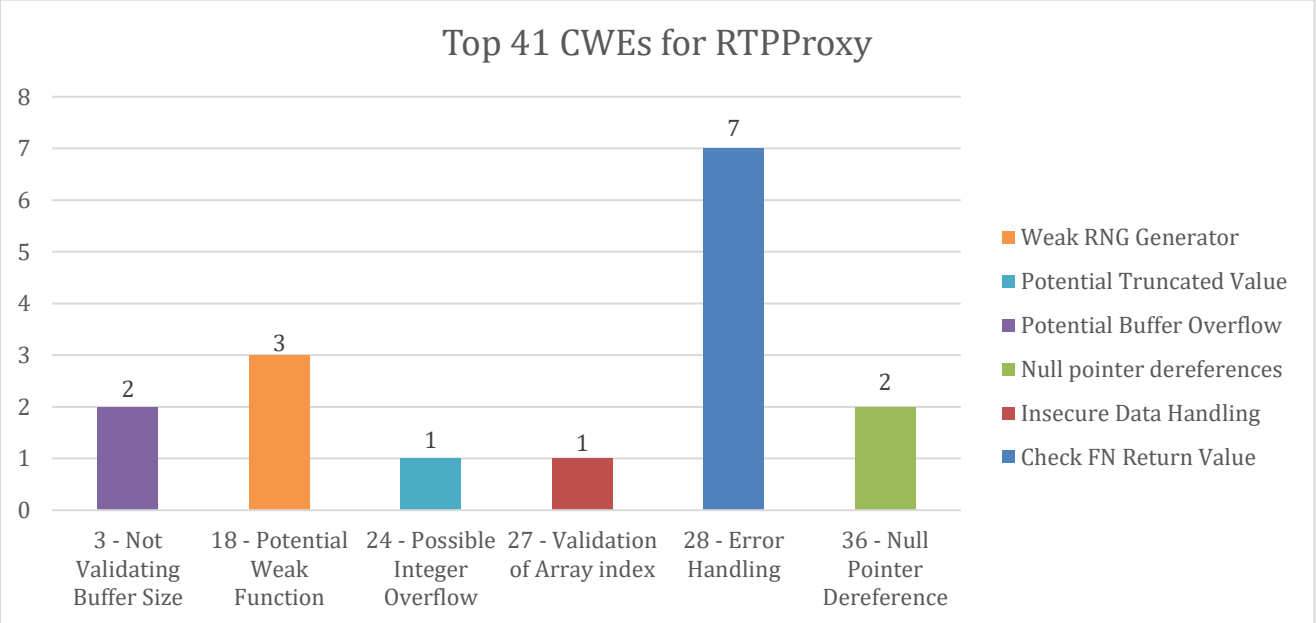


Chart 8

Chart 9 Below summarizes the SANS Top 25 and the SANS on the cusp (26-41) Common Weakness Enumerators found in the StrongSwan component of the product.

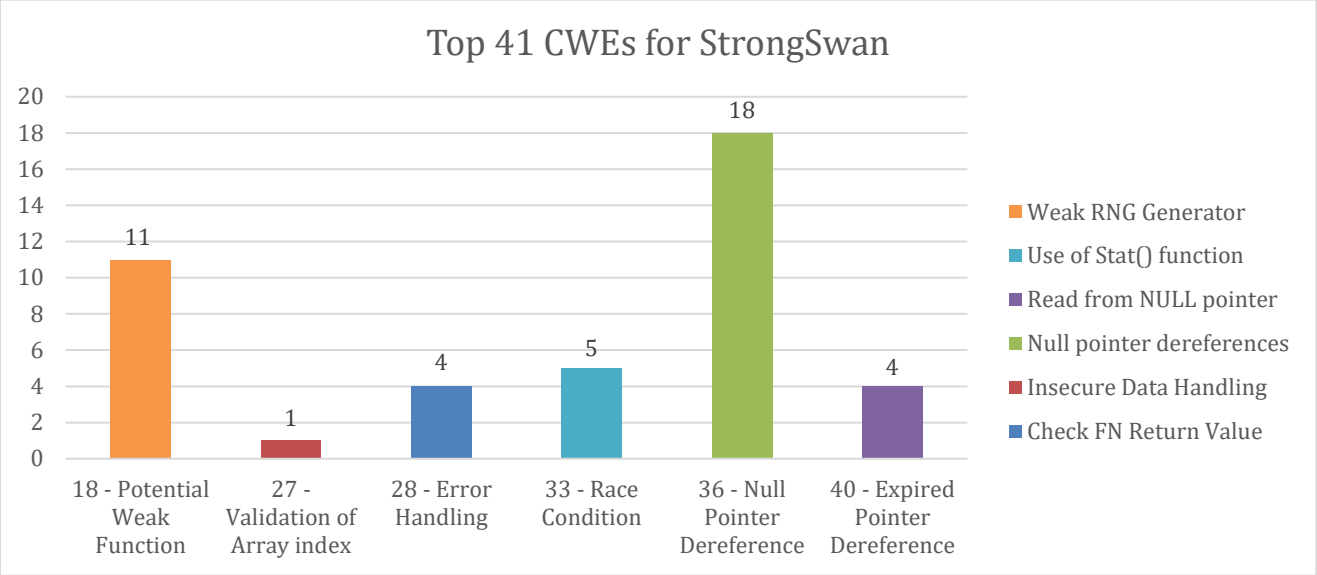


Chart 9

RISK ASSESSMENT AND STRUCTURED PENETRATION TESTING

The Community of Trust Corporation provided a detailed risk analysis and a detailed Risk Profile Report on the product. UL LLC, using the data obtained from evaluating and assessing the product, specifically from results in Malformed Input Testing, Known Vulnerability Testing, Static code, binary and byte code analysis; performed a structured penetration testing of the product. Penetration testing was carried out on the product in order to probe for vulnerabilities in the product. Attempts were made to identify system, application and service information via scanning of the ports, interfaces and services. Use of that information was considered in attempts to circumvent the security measures of the product. Exploit tools and scripts were used for discovered information to attempt to access the product, elevate the privilege once accessed or to gain further information about the product.

Some of the following tools used in the Structured Penetration Testing Assessment and a summary of the test results are described in Table 9:

Tool Name	Tests Summary
NMAP v7.01 I586-pc-linux-gnu	We were unable to circumvent the risk controls of the product.
IKE-SCAN v1.9 I586-pc-linux-gnu	We were unable to circumvent the risk controls of the product.
	Unable to circumvent the authentication risk controls and therefore unable to elevate privilege on the product.
NETDISCOVER Version 0.3-beta7 I586-pc-linux-gnu	We were unable to circumvent the risk controls of the product.
IKEPROBE.EXE	We were unable to circumvent the risk controls of the product.

Version 0.1beta I586-pc-linux / WINE Framework	Unable to circumvent the authentication risk controls and therefore unable to elevate privilege on the product.
WINE v 1.9.4 I586-pc-linux	We were unable to circumvent the risk controls of the product.
NEXPOSE v 6.0 Linux	We were unable to circumvent the risk controls of the product.
	Unable to access or authenticate on the product via unauthorized means.
	Unable to exploit CVEs that were found in the product and described in the risk analysis by the vendor as either closed or not relevant.
	Unable to circumvent the authentication risk controls and therefore unable to elevate privilege on the product.
METASPLOIT PRO v 4.11.6 Linux	We were unable to circumvent the risk controls of the product.
	Unable to access or authenticate on the product via unauthorized means.
	Unable to exploit CVEs that were found in the product and described in the risk analysis by the vendor as either closed or not relevant.
	Unable to circumvent the authentication risk controls and therefore unable to elevate privilege on the product.
	Attempts to exploit using POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks. All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable. Unable to take advantage of the protocol version negotiation feature built into SSL to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session.
	ISC BIND handling TKEY queries can cause named to exit allowing remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries. Unable to be successful in exploit and no login credentials were obtained.
	Attempt man-in-the-middle attacks using ChangeCipherSpec messages to trigger use of a zero-length master key in certain communications, and hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability. Unable to be successful in exploit and no login credentials were obtained..
DEFENSICS v 11.10.12 Windows	We were unable to circumvent the risk controls of the product.
	We were able to get the product to be in a denial of service for a maximum of 15 seconds but the product recovered after the test.

Table 9

UL 2900 TESTING COMPLIANCE SUMMARY

The following Table 10 describes an assessment and evaluation as a summary of the sections of UL 2900-1.

- COMPLIED WITH THE REQUIREMENTS OF UL2900-1 MARCH 30TH 2016
- NON-COMPLIANCE WITH THE REQUIREMENTS OF UL 2900-1 MARCH 30TH 2016

Compliance Summary	Status
DOCUMENTATION OF PRODUCT, PRODUCT DESIGN AND PRODUCT USE	
PRODUCT DOCUMENTATION	
PRODUCT DESIGN DOCUMENTATION	
DOCUMENTATION FOR PRODUCT USE	
RISK CONTROLS	
GENERAL	
ACCESS CONTROL, USER AUTHENTICATION, AND USER AUTHORIZATION	
REMOTE COMMUNICATION	
CRYPTOGRAPHY	
PRODUCT MANAGEMENT	
RISK MANAGEMENT	
VENDOR PRODUCT RISK MANAGEMENT PROCESS	
VULNERABILITIES AND EXPLOITS	
KNOWN VULNERABILITY TESTING	
MALWARE TESTING	
MALFORMED INPUT TESTING	
STRUCTURED PENETRATION TESTING	
SOFTWARE WEAKNESSES	
SOFTWARE WEAKNESS ANALYSIS	
STATIC SOURCE CODE ANALYSIS	
STATIC BINARY AND BYTE-CODE ANALYSIS	

Table 10

END OF DOCUMENT