International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(2): 111-118
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

A research study: Usage of RC4 stream cipher in SSL configurations of web servers used by Sri Lankan Financial Institutes

T.D.B Weerasinghe* and Chamara Disanayake
CICRA Campus, Colombo 4, Sri Lanka
tharindu.weerasinghe@gmail.com
chamara@nic.lk

ABSTRACT

The security of the Internet is mainly based on Secure Socket Layer (SSL) or its successor Transport Layer Security (TLS). To secure the on-line transactions, the organizations widely use the particular protocol(s) in their web portals. In SSL, a lot of cipher suits are used as encryption algorithms. RC4 is the most commonly used stream cipher (although it is regarded as a weak cipher) and it is used in SSL as an encryption algorithm. SSL is the most renowned security protocol for pursuating a secure link between a web server and a browser. Nonetheless the stream cipher RC4 is found to be vulnerable for various attacks. The main objective of this research study is to find-out the usage of RC4 stream cipher in on-line web portals of Sri Lankan Financial Sector, as well as the awareness level of the IT and Security administrators and managers of some of the selected banks which are geographically based in Sri Lanka, regarding the usage of RC4 in SSL.

KEYWORDS

RC4, SSL, Stream Cipher, Web Portals, Sri Lankan Financial Institutes

1 INTRODUCTION

Even though there are proven scenarios that illustrate RC4's vulnerabilities in SSL, a lot of Sri Lankan banks were using RC4 as one of the cipher suits in the SSL configurations of their respective on-line web portals. This was identified by the SSL testing tools available in open literature. By the time this case/research study started many of the private banks in Sri Lanka were not updated to the latest of SSL/TLS versions. And hence why they were vulnerable to RC4 based attacks. Most of the vulnerabilities occur due to the Invariance Weakness of the particular algorithm. One of the other objectives of this study was to know the awareness level of the System Administrators, IT Managers and IT Administrators in the financial sector in Sri Lanka, about the RC4 cipher vulnerabilities in SSL. A questionnaire (presented later in this paper) was given to some of the selected professionals mentioned above. The outcomes of the survey are depicted in the results section.

2 LITERATURE

WWW (World Wide Web) is the largest network around and information is spread to every corner of the world through the World Wide Web which we call as the Internet. Nowadays most of the professionals can't survive in their professions if they don't have the Internet access. When information spreads everywhere the privacy and secrecy of information also pay a vital role. When Information become paramount, the protection of information becomes even more important; hence the secure information transactions are encouraged over the Internet. The Internet is browsed or surfed through web browsers (e.g. Chrome, Firefox, Internet Explorer, Opera etc). The web browsers render the web-pages a nd illustrate them to the users. It is self explanatory that the vital (sensitive) information are transferred via web browsers hence the information should be transferred through secure channels. To protect (or encrypt) the sensitive information over the Internet via web browsers, there is a standard mechanism called SSL (Secure Socket Layer) through handshakes and agreed protocols the information will be encrypted by SSL and transformed over the Internet. A man in the middle can intercept but can only get the meaningless data which are encrypted. SSL uses various ciphers to encrypt the data/information; likes of RSA, AES, RC4 etc.

The financial sector as well the enterprise web applications use SSL in order to make their application transactions secure. In Sri Lanka also a lot of financial institutions use HTTPS. When you use SSL (specially the versions prior to TLS1.2) and if you have configured the stream cipher RC4 as a cipher in SSL then you are vulnerable to some attacks which are mainly based on the in-variance weakness of the RC4 algorithm.

2.1 Stream Cipher

In cryptography, the Stream Cipher is a light weight cipher which encrypts plain-text bit by bit. Input plain-text is considered as a bit stream and that stream is encrypted using a key which can be used to decrypt the particular cipher text and obtain the plain text. Stream ciphers are widely used in embedded systems because they are light weight. Unlike block ciphers stream ciphers are less secured. Among all the stream ciphers, the most popular one is RC4.

2.2 RC4 Stream Cipher

RC4 (originally named as Rivest Cipher 4 or ARC4, founded by Ron Rivest at RSA Security), is the well-known stream cipher around which is widely used in applications like WPA, SSL, TLS, Kerberos, PDF and Skype [4].

Here, the algorithm RC4 is described with respect to its major parts:

The Key Scheduling Algorithm (KSA) and the Pseudo- Random Generation Algorithm (PRGA). In most of the applications RC4 is used with a word size 8 (n = 8) and array size N = 2^8 [6]

KSA:

```
for i = 0 to 255
  S[i] = i;
end for
j=0
for i = 0 to 255
  j = (j+S[i]+K[i mod keylength]) mod
256;
  swap S[i] and S[j];
end for
```

PRGA:

```
i = 0, j=0;
for x = 0 to L-1
   i = (i+1) mod 256;
  j = (j+S[i]) mod 256;
  swap S[i] and S[j];
  GeneratedKey = S[ (S[i] + S[j]) mod
256]
  Output = M XOR GeneratedKey
end for
```

Where ‘M[]’ is the plain-text message and L is its length. Keylength is the initial key length in bytes.[6]

2.3 SSL

SSL (Secure Sockets Layer) is considered to be the standard security methodology for establishing an encrypted communication link between a web server and a browser. SSL is an industry standard which is used by many websites to safeguard their on-line transactions with their stakeholders. In other words, SSL is the standard technology for maintaining a secure Internet connection and protecting sensitive data that is being shared between two entities or systems, preventing eavesdroppers/hackers from reading and amending any information transferred, including the personal information of the users. The two entities or systems can be a server and a client (e.g. an on-line shopping wen site and a browser) or server to server (e.g. an application with sensitive personal identifiable data or information with salary details of the employees of an organization). It achieves this by encrypting the data shared between the two systems. It uses encryption algorithms such as AES, 3DES, RC4 and Hash Functions to scramble the data in transit and preventing hackers from reading it as it is sent over the connection. This information can be anything sensitive or personal which can include personal civil information, bank account details, credit card numbers and other valuable contact information. TLS (Transport Layer Security) is regarded as a successor to SSL, a more secure and trusted version of SSL. The computer world still refers to the security certificates as SSL because it is a more commonly used term. [6].

2.4 How does SSL work

1. A browser or server tries to connect to a Website, in other words, a client attempts to connect to a Web server, secured with SSL. The particular browser or the server requests the identity of the Web Server itself.

2. The Web server sends the browser or the server a copy of its SSL certificate.
3. Then the particular browser or the server checks whether the SSL certificate can be trusted or not. If trusted then, it sends a message to the Web server.

4. After that, the Web Server sends back a digitally signed acknowledgment to start a SSL encrypted session.

5. Encrypted data is shared between the browser or the server and the Web server.

2.5 How RC4 is used in SSL

RC4 is used in SSL Record Protocol for encryption in many SSL cipher suites. In the Handshaking Protocol, RC4 encryption keys are generated for upstream and downstream communication. In the Record Protocol, the upstream key is used for encryption of the client-to-server communication, whereas the downstream key is used for encryption of the server-to-client communication. It is important to note that the encryption(s) are state-full, using the first key-stream bytes for encrypting the first message, the succeeding key-stream bytes for encrypting the next message, etc.

2.6 Vulnerabilities in RC4 in SSL

Several researchers and experts have proved that RC4 is vulnerable for attacks in SSL. Implementation of RC4 (the structure of the algorithm) itself found to be vulnerable. Statistical biases in the pseudo-random number generator (PRNG) as well as some in the key stream generator (KSA) that lead an attacker to distinguish RC4 from random and to guess or predict its allegedly pseudo-random bits with a higher probability. On the other hand, a lot vulnerabilities occur due to the in-variance weakness of the RC4 algorithm [2].

2.7 In-variance Weakness of RC4

Invariance Weakness is about a pattern which can be derived in the key-stream. It is described as an L-shape key pattern in RC4 keys; if further explained, once it exists in an RC4 key, keeps part of the state permutation intact throughout the initialization process. This intact part includes
the least significant bits of the permutation, when processed by the Pseudo Random Number Generator (PRNG) algorithm, it determines the least significant bits of the allegedly pseudo-random output stream along a long prefix of the stream. These biased stream bytes are XOR-ed with the plain-text bytes, resulting in significant leakage of plain-text bytes from the cipher-text bytes.[2]

These patterns are formed for different number of Least Significant Bits (LSBs), a single LSB, 2 LSBs, 3 LSBs to 7 LSBs, resulting with different classes of weak RC4 keys. Because of the structure of these classes, each class contains
the succeeding classes and thus the first class is the largest, denoted below as the Main Class. The portion of q-class for L byte keys (which is the probability of a random key to be in the class) is 2 -(qL+(9-q)). For 16-byte key the portion of the Main Class (1-class) is 2 -24 (1 in 16 million) and the portion of 2- class is 2 -39 (very rare). Several researchers have found that the Invariance Weakness of RC4 has several crypt-analytic applications, including statistical biases in the RC4's PRNG that allow an eavesdropper to distinguish RC4 streams from randomness and enhancement of trade-off
attacks on RC4. Another application of the Invariance Weakness, is the leakage of plain-text data into the cipher-text when q-class keys are used, which is described in [2].

Given the fact that the Invariance Weakness is exposed only in the initial 100 bytes of the key-stream, it can be used only for the initial 100 bytes of the secured upstream traffic and the first 100 bytes of the secured downstream traffic.
Given the fact that the first encrypted message in each direction is the SSL Handshake Finished message (36-bytes in a typical usage of SSL), about 64 bytes of secret plain-text data are vulnerable for attacks [2].The attack described in the research published by www.imperva.com is based on sniffing a large number of SSL connections encrypted with RC4, waiting for the arrival of a weak key. Once a weak key
arrives, the attacker is good enough to predict the LSBs of the key-stream bytes, and he/she uses these to extract the LSBs of the plain-text bytes

from the cipher-text with significant advantage. In order to achieve this situation, the attacker needs to determine which SSL sessions are the ones in which weak keys were used. For this isolation, the attacker can use the fact that the first encrypted bytes include the SSL “Finished” message and HTTP request, both having predictable information. Thus, when a weak key is used, the plain-text patterns are XOR-ed with key-stream patterns, generating cipher-text patterns visible to the attacker.
`

2.8 Sri Lankan Financial Institutes

In this study, the Sri Lankan financial domain which consists of the Banking Sector and other Financial Institutes, taken into consideration. There are 32 Commercial and Licensed Specialized banks and 45 Registered Financial Institutes in Sri Lanka [12, 13, 14]. Almost all these banks use cooperate websites and also customer log-in portals. Hence SSL/TLS is playing a basic vital role. Nonetheless, one of main objectives of this research was to identify the awareness level of the IT System Administrators and Network Engineers of these banking/financial sector, regarding RC4's vulnerabilities in SSL and also how well the particular institutes' web based products are protected against them.

2.9 Mitigation of RC4 vulnerabilities in SSL

One of the solutions is to upgrade SSL into TLS1.2 where the stream cipher RC4 algorithm is not used as a cipher suit. This is the solution that a lot of banks have adhered to, during the research. Please note that, by the time the research started, a lot of banks were using the RC4 as a cipher suit (analyzed using the online tool, SSL Server Test, Powered By Qualys SSL Labs). The other is to disable RC4 Cipher Suit in the SSL configuration of the web server [8].

3 RESEARCH METHODOLOGY

3.1 Preliminary Research Method

A study of the existing RC4 vulnerabilities and remedies was carried out in-terms of finding the reliable and suitable remedies.

Data were gathered via a Survey (Google Forms were used to gather data) from the senior professionals of some of the Sri Lankan Banks. The aim of the survey was the identify the background knowledge and awareness of the IT-Security Admins and Managers of Sri Lanka Banks, about the RC4 cipher vulnerabilities in SSL/TLS. In open literature, researchers, professionals in the domain have already discussed about these vulnerabilities but it is important to know to which extend the Sri Lankan professionals in the domain, are aware of these. The questionnaire was prepared to cover a wide range of areas related to SSL, RC4 and opinions of the organizations.

Then the SSL protocols used by the targeted web sites were analyzed using the online tools available.

https://www.ssllabs.com/ssltest is used which is publicly available to anyone interested.

3.2 Action plan

- Selection of Methods and Tools
- Identification and illustration of the vulnerabilities in SSL when using RC4.
- Analysis of the suitable remedies.
- Preparation of the questionnaire for Data Collection
- Circulation of the questionnaire to the selected professionals and data gathering.
- Data Analysis.

4 RESULTS AND ANALYSIS

- Twelve senior level employees from several banks of Sri Lanka were contacted and inputs were taken for the questionnaire.
- All of them know RC4 Cipher and also all of them know that SSL has RC4 as a cipher suit.

- 75% of them know that RC4 is vulnerable in SSL.
- 75% of their institutes use SSL and all of them has mitigated RC4. Summary of Results are shown in respective pie charts:

Summary of Results are shown in respective pie charts:

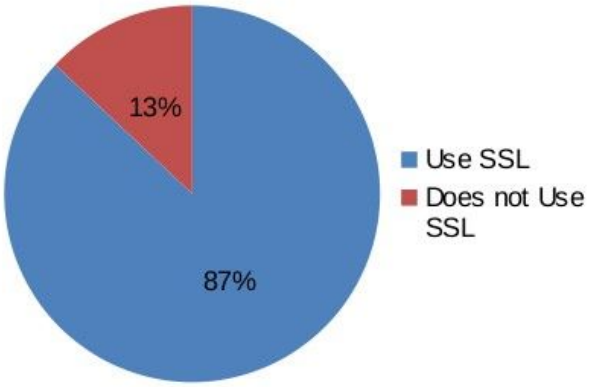

Figure 1. SSL usage in the customer login portals of the Sri Lankan banks (by June 2017)

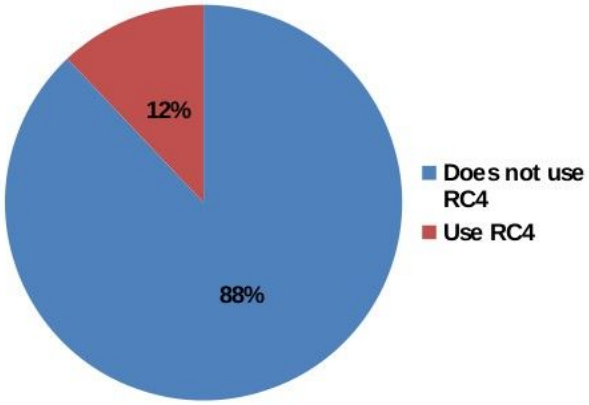

Figure **2.** RC4 cipher suit usage in SSL configurations of the customer login portals of the Sri Lankan banks (by June 2017)

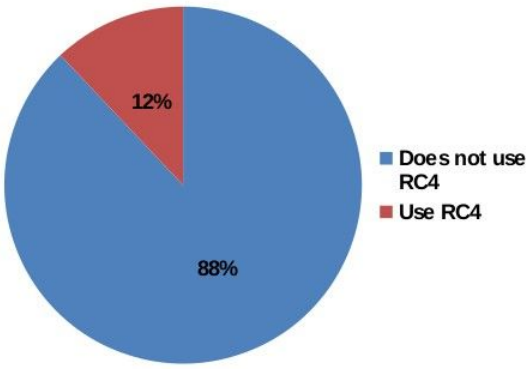

Figure 3. RC4 cipher suit usage in SSL configurations of the customer login portals of other financial institutes of Sri Lanka (by June 2017)

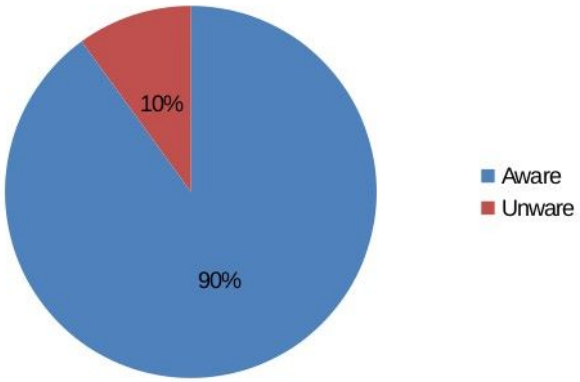

Figure 4. Awareness levels of the selected IT Infrastructure/ Networking professionals in Sri Lankan Banks about RC4 usage in SSL

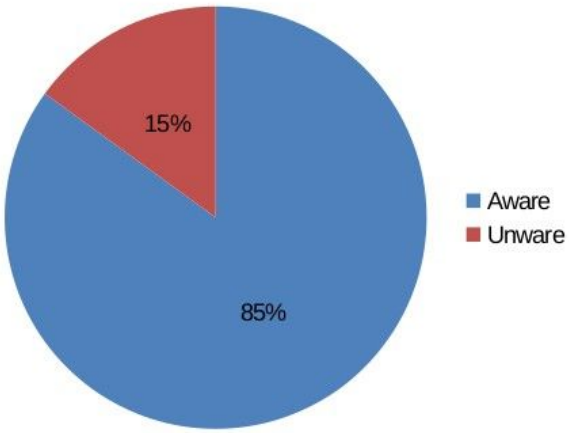

Figure **5.** Awareness levels of the selected IT Infrastructure/ Networking professionals in Sri Lankan Banks about RC4 vulnerabilities in SSL

Results of finding a suitable remedy for Sri Lankan eBusiness sector if the stakeholders still use RC4 cipher suit in their web servers :

Upgrading to TLS1.2 which is the latest of TLS and this needs management approval. This is about shifting/changing infrastructure. Well this is not hard but if there are management decisions (highly unlikely) then an organization will have to hold back in changing.

JDK8 supports TLS by, default. Support for TLS 1.2 initially appeared in JDK 7 in 2011 [9, 10, 11].

Setting up JDK 8 to use TLS 1.2 as the default is good because of two reasons:

1. TLS1.2 is backward compatible means even after upgrading to TLS1.2 you can use even TLS1.0.

2. Few systems will be affected by this unless configured to use an algorithm that was removed for security reasons [10].

For other versions of SSL, it is recommended to disable RC4 as mentioned in the Introduction. Sample connector entry in the server.xml of Apache Tomcat 8.0.41 is mentioned here:

Remedy apart from upgrading to TLS1.2:

```
<!ENTRY STARTS>
<Connector
protocol="org.apache.coyote.http11.Http
1
1
NioProtocol"
port="8443" maxThreads="200"
scheme="https" secure="true"
SSLEnabled="true"
keystoreFile="/usr/lib/jvm/java8oracle
/
bin/keystore"
keystorePass="SetFree123"
clientAuth="false" sslProtocol="TLS"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CB
C_S
HA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,RC4
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_RC4_128_SHA
"/>
<!ENTRY FINISHES>
```

5 CONCLUSION

Nearly 75% of the Banks and Financial Institutes in Sri Lanka have been transferred to TLS1.2 from SSL and TLS older versions and hence they have mitigated the RC4 vulnerabilities (this has happened after April 2017, because when by the time the research study commenced, most of the banks had not been upgraded and hence they were using RC4. Nonetheless, the other 25% is under a risk of exposing major part of the plain-text messages as they use the RC4cipher suit in their SSL configuration. TLS1.2 was not used by the most of the Sri Lankan banks until March 2017 (by the time this research started, they were not using TLS1.2 and hence they were vulnerable to RC4 weaknesses in SSL. It is very interesting to see that, during the research period, most of the banks have shifted to TLS1.2 to mitigate RC4 like vulnerabilities. RC4 stream cipher is understood to be a weak cipher suit in SSL and it is recommended that it is disabled in all SSL and TLS versions if the organizations does not use TLS1.2 or above. Java 8 (JDK 8) supports TLS by default and hence Apache 8.0.44 also supports TLS. As a best practice,when you harden your web servers it is good to use the latest versions available; of course you need to have the management approval for this kind of an infrastructure change; but it is essential to convince the management use the best practices.

According to the results, the majority of the selected IT Administrators of the selected Banks (75% of them) are aware of the RC4 vulnerabilities.

For the Banks and Financial Institutes that are yet to avoid RC4 vulnerabilities which are mainly caused due to the Invariance weakness of the cipher, it is recommended to migrate to TLS1.2 which has no RC4 cipher suit or else at-least remove RC4 cipher suits from their SSL cipher configuration. As far as the objectives of this research are concerned, it is clearly depicted that all of those objectives are achieved with

results and there are no any motive or thought to publish the research data publicly, as they are regarded as very sensitive in-terms of banking and financial industry. If there is a formal and legal request the researcher can provide the necessary details to the authorized person or institute. The tools used to check the vulnerabilities and it is worth using such tools get an idea about the security standard of the web sites of your organization.

REFERENCES

1 “What is SSL?,” What is SSL? [Online]. Available: http://info.ssl.com/article.aspx?id=10241. [Accessed: Jan & Feb -2017].

2 IMPERVA., “Attacking SSL when using RC4.” Hacker Intelligence Initiative, Mar-2015.

3 “DigiCert® Certificate Inspector: Vulnerabilities,” DigiCert. [Online].Available: https://www.digicert.com/certinspector-vulnerabilities.htm. [Accessed: Jan-2017].

4 “RC4,” Wikipedia, 02-Jul-2017. [Online]. Available: https://en.wikipedia.org/wiki/RC4

5 “What is SSL, TLS and HTTPS?,” What is SSL, TLS and HTTPS? Symantec. [Online]. Available: https://www.symantec.com/page.jsp?id=ssl-information-center. [Accessed: June-2017].

6 Y. Nawaz, K. Gupta, and G. Gong, “A 32-bit RC4-like Keystream Generator.” International Association for Cryptologic Research, 2005.

7 How Does SSL Work? What is SSL? | Entrust. (n.d.). Retrieved June 24, 2017, from https://www.entrust.com/ssl

8 “WHICH SSL/TLS PROTOCOL VERSIONS AND CIPHER SUITES SHOULD I USE?,” WHICH SSL/TLS PROTOCOL VERSIONS AND CIPHER SUITES SHOULD I USE? [Online]. Available:https://securityevaluators.com/knowledge/blog/2015 0119-protocols/. Accessed: June-2017].

9 B. S. Inc, “Finding and Fixing Vulnerabilities in SSL RC4 Cipher Suites Supported , a Medium Risk Vulnerability,” Beyond Security - Vulnerability Assessment and Management.Online].Available:http://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_ssl_rc4_cipher_suites_supported. [Accessed: June-2017].

10 G. Author, “JDK 8 will use TLS 1.2 as default,” JDK 8 will use TLS 1.2 as default | Oracle. [Online]. Available: https://blogs.oracle.com/java-platform-group/jdk-8-will-usetls- 12-as-default. [Accessed: June-2017].

11 H. Schlawack, “Hardening Your Web Server's SSL Ciphers,” Homepage and blog of Hynek Schlawack, 12-Jun-2017 [Online].Available: https://hynek.me/articles/hardeningyour-web-servers-ssl-ciphers/. [Accessed: June-2017].

12 “Licensed Commercial Banks,” Licensed Commercial Banks. [Online]. Available: http://www.cbsl.gov.lk/htm/english/05_fss/popup/licensed_cb.htm.

13 “Licensed Specialised Banks,” Licensed Specialised Banks. [Online]. Available: http://www.cbsl.gov.lk/htm/english/05_fss/popup/licensed_sb.htm.

14 “Licensed Finance Companies,” Registered Finance Companies. [Online]. Available: http://www.cbsl.gov.lk/htm/english/05_fss/popup/registered_fc.htm.

APPENDIX

Questionnaire given to the target audience:

1. Does your institute use SSL in your cooperate web site and also in customer login portals?

Options:
Yes
No

1.1 . If the answer for the above question is “No” then do you think your management will bring SSL into picture in near future?

Options:
Yes
No

1.2 . If the answer for the above question (1.1) is “No” then don't you think that your cooperate web site can be compromised by an attack?

Options:
Yes
No

2. Do you know about the stream cipher RC4?

Options:
Yes
No

2.1 . Do you know that SSL uses RC4 as an encryption algorithm?

Options:
Yes
No

2.1 . Are you aware of the vulnerabilities of RC4 in SSL?

Options:
Yes
No

2.1.1 If yes, then can you list some of them?
Please write down a few

3. Are you aware of the existing remedies for the above vulnerabilities?

Options:
Yes
No

3.1. If yes, then what are the remedies for the above vulnerabilities that you are aware of?
Please write down a few

4. If your organization is yet to mitigate the RC4 vulnerabilities, then what are the reasons for that according to your opinion.
Please write down a few

5. If your organization already mitigated the above vulnerabilities, then who was behind that and what made you to mitigate them?
Please write down a few

5.1 Given the fact that your organization has migrated to TLS1.2; when did it happen?