

**ASSIGNMENT**

**TECHNOLOGY PARK MALAYSIA**

**AICT006-4-2-DSF**

**DIGITAL SECURITY AND FORENSICS**

**UCDF2107ICT(SE)**

**TASK 1**

**HAND OUT DATE: 13 APRIL 2023**

**HAND IN DATE: 22 MAY 2023**

**WEIGHTAGE: 40%**

**INSTRUCTIONS TO CANDIDATES:**

1. **Submit your assignment at the administrative counter.**
2. **Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).**
3. **Late submissions will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.**
4. **Cases of plagiarism will be penalized.**
5. **The assignment should be bound in an appropriate style (comb bound or stapled).**
6. **Where the assignment should be submitted in both hardcopy and softcopy, the softcopy if the written assignment and source code (where appropriate) should be on a CD in an envelope / CD cover and attached to the hardcopy.**
7. **You must obtain 50% overall to pass this module.**

Table of Contents

[**1.0 INTRODUCTION 1**](#_Toc135315844)

[**2.0 SCANNING METHOD AND TOOL SELECTION 2**](#_Toc135315845)

[**2.1 Scanning Method 2**](#_Toc135315846)

[**2.2 Tool Selection 3**](#_Toc135315847)

[**3.0 VULNERABILITY IDENTIFICATION 11**](#_Toc135315848)

[**3.1 Vulnerability 1: SSL Version 2 and 3 Protocol Detection (Sin Lian Feng TP065298) 11**](#_Toc135315849)

[**3.1.1 Identification 11**](#_Toc135315850)

[**3.1.2 Justification 13**](#_Toc135315851)

[**3.2 Vulnerability 2: MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (Bernard Ong Yuzhe, TP065754) 18**](#_Toc135315852)

[**3.2.1 Identification 18**](#_Toc135315853)

[**3.2.2 Justification 20**](#_Toc135315854)

[**3.3 Vulnerability 3: MS09-22: Vulnerabilities in Window Print Spooler Could Allow Remote Code Execution (961501) (She Jun Yuan TP065157) 22**](#_Toc135315855)

[**3.3.1 Identification 22**](#_Toc135315856)

[**3.3.2 Justification 24**](#_Toc135315857)

[**3.4 Vulnerability 4: MS10-009: Vulnerabilities in Windows TCP/IP could allow Remote Code Execution (974145) (Teoh Mae Kay TP065097) 27**](#_Toc135315858)

[**3.4.1 Identification 27**](#_Toc135315859)

[**3.4.2 Justification 29**](#_Toc135315860)

[**3.5 Vulnerability 5: MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318) (Tay Hui Yee TP064988) 34**](#_Toc135315861)

[**3.5.1 Identification 34**](#_Toc135315862)

[**3.5.2 Justification 36**](#_Toc135315863)

[**4.0 CONCLUSION 39**](#_Toc135315864)

[**5.0 REFERENCES 40**](#_Toc135315865)

**TABLE OF FIGURES**

[Figure 1: Nessus Logo (Tenable, 2019) 3](#_Toc135367745)

[Figure 2: Open VMware Workstation Pro 5](#_Toc135367746)

[Figure 3: Enter password to login Window 2008 5](#_Toc135367747)

[Figure 4: Press command prompt 6](#_Toc135367748)

[Figure 5: Find Windows 2008 victim machine’s IP address. 6](#_Toc135367749)

[Figure 6: Key in username and password to login to Nessus 7](#_Toc135367750)

[Figure 7: Press “New Scan” button 7](#_Toc135367751)

[Figure 8: Press “Advanced Scan” 8](#_Toc135367752)

[Figure 9: Fill in scanning details 8](#_Toc135367753)

[Figure 10: Fill in the username and password 9](#_Toc135367754)

[Figure 11: Press Play Button 9](#_Toc135367755)

[Figure 12: Result of the vulnerability scan 10](#_Toc135367756)

[Figure 13: SSL Version 2 and 3 Protocol Detection Vulnerability 11](#_Toc135367757)

[Figure 14: 4 Layers In The SSL Protocol Stack (Bhakhra, 2023) 12](#_Toc135367758)

[Figure 15: SSL Handshake Protocol (Bhakhra, 2023) 14](#_Toc135367759)

[Figure 16: Original Handshake Protocol Message (Wagner & Schnier, 1996) 16](#_Toc135367760)

[Figure 17: Handshake Protocol Message Exploited By Attackers (Wagner & Schnier, 1996) 16](#_Toc135367761)

[Figure 18: MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution 18](#_Toc135367762)

[Figure 19: DNS Architecture (Datadog, 2022) 19](#_Toc135367763)

[Figure 20: MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501) 22](#_Toc135367764)

[Figure 21: Windows Print Spooler (Makwana, 2021) 23](#_Toc135367765)

[Figure 22: Reconnaissance 26](#_Toc135367766)

[Figure 23: MS10-009: Vulnerabilities in Windows TCP/IP could allow Remote Code Execution (974145) 27](#_Toc135367767)

[Figure 24: IPv6 Router Advertisement Message (Network Academy.io, 2020) 31](#_Toc135367768)

[Figure 25: MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318) 34](#_Toc135367769)

**LIST OF TABLES**

[Table 1: Comparison table between Nessus and Nmap (Nmap vs Nessus | Learn the Top Key Differences and Comparisons, 2021) 4](#_Toc135255235)

# INTRODUCTION

Vulnerability Assessment (VA) is a critical process that helps security professionals to find and fix system vulnerabilities. They can create efficient defenses against attacks and risk reduction strategies by carefully analysing potential vulnerabilities. By proactively identifying and fixing potential entry holes for hostile actors, VA's primary goal is to improve the overall security posture of an organisation.

In this analysis, we'll go into great detail about how scanning technologies are used to find vulnerabilities in the Windows Server 2008 operating system in particular. In order to do this, we make use of virtual machines, which give us a regulated and separated environment where we can conduct tests without affecting the production environment. Security experts can recreate real-world situations and assess the system's vulnerability to different assaults by using virtual machines.

Each vulnerability will be carefully explored to ensure an in-depth understanding of its characteristics and potential impacts. We will look into the existence of these flaws and highlight the strategies used by attackers to take advantage of them. Security experts can create effective responses and strengthen the system's defences by getting knowledge into the methods and strategies used by hackers.

This assessment will also include specific examples of how these vulnerabilities have been used in real-life situations, rather than just focusing on theoretical issues. We can learn a lot about the potential effects and the impact assaults may have on an organization's operations, data integrity, and reputation by examining actual cases of attacks.

This examination seeks to give security professionals a comprehensive understanding of potential risks by going into the depths of vulnerability assessment and carefully examining each discovered vulnerability. With all the information, the security professionals can decide with confidence whatever safety precautions and security measures to put in place to give their organisation the best level of protection.

# SCANNING METHOD AND TOOL SELECTION

## Scanning Method

Vulnerability scans are essential for defending assets from attack by spotting outdated software, misconfigurations, and other typical security problems. Vulnerability scanning tools were initially created to test local networks and devices which have developed to include the contemporary IT environment as well as specialized tools for certain assets, applications, and vulnerabilities (Kime, 2023). There are various types of scanning methods, which are port scanner, web application vulnerability scanner, network vulnerability scanner, host-based vulnerability scanner, database scanner, source code vulnerability scanner, cloud vulnerability scanner, and others (RSI Security, 2023). The scanning method that has been used for this assignment is **network scanning**. Network scanning involves the systematic search for vulnerabilities in the system's active devices. By incorporating one or more traits in the network protocol, it discovers and analyses the connected devices. These features actively detect the signals of the vulnerability and provide insights into the network's security state. It significantly simplifies the system maintenance, monitoring, and security evaluations. When utilized effectively, network scanning may provide valuable information on the top defenses against networks-based cyberattacks (Odogwu, 2021).

## Tool Selection

In order to conduct vulnerability scanning on the Windows Server 2008 victim machine, a tool for scanning vulnerability will be selected. There are a tons of scan tools that can be used for scanning the vulnerabilities of the Windows Server 2008 victim machine, which is Nessus, Nmap, OpenVAS and others. The vulnerability scanning tool that have been chosen is **Nessus**. Nessus is a proprietary vulnerability scanner that was created by Tenable, Inc. It is also an open-source network vulnerability scanner, which use the Common Vulnerabilities and Exposures architecture to make it simple for compliant security solutions to cross-link with one another (Itperfection, 2021). However, Nessus should be known as just one small component of a sound security strategy, rather than a comprehensive security solution. Nessus is also merely a tool that scans the systems for weaknesses that hackers COULD use, and it does not actively prevent attacks from the hacker (Wendlandt, 2019).

A blue text on a black background

Description automatically generated with low confidence

Figure : Nessus Logo (Tenable, 2019)

Below is the table for comparison table between Nessus and Nmap.

|  |  |
| --- | --- |
| **Nessus** | **Nmap** |
| The first vulnerability scanner employed to identify the system's flaws. | a port discovery tool that is used to find active hosts on a network and for host detection. It can also be used to determine the operating system and database version running on our server. |
| famous for its vulnerability scanning skills, comparable to Nmap in that it searches ports and targets known flaws on a system when evaluating a specific host. | a powerful port scanner that utilizes network scanning to find the active host. Once it is done, Nmap will collect the information about the open ports on those hosts. |
| Better software that refers to testing the system's incapacity. | Achieve better network performance involves efficiently finding the IP network infrastructure. |
| simply serves as a tool to check for vulnerabilities and aid in problem-solving; it does not actively defend against assaults. | can defend the system against intrusion. |
| enabling users to choose which machines should be scanned during scans. | can be used to keep an eye on both a small network and a single host. |

Table : Comparison table between Nessus and Nmap (Nmap vs Nessus | Learn the Top Key Differences and Comparisons, 2021)

Based on the comparison table above, the reason of choosing Nessus as the vulnerability scanning tools to scan the vulnerability of the Windows 2008 victim machine is that Nessus offers more suitability when compared to the Nmap as Nessus provides the ability to evaluate the severity level of the identified vulnerabilities that contained in the Windows 2008 victim machine. Besides, Nessus also provides the potential solution to address the vulnerabilities. With the solutions that provided by Nessus, it allows users to have the actionable insights on how to effectively solve the vulnerabilities that present in this victim machine. It also provides detailed description about the specific vulnerability so that the user can gain deeper understanding about the vulnerability.

**Steps to Scan Vulnerability by Using Nessus**

VMware Workstation Pro will be used to open the Windows 2008 victim machine to get the IP address that will be used for scanning the vulnerabilities by using Nessus. Below are the steps to scan vulnerability by using Nessus.

A screenshot of a computer

Description automatically generated

Figure : Open VMware Workstation Pro

The first step of scanning the vulnerability of the Windows 2008 is to open the VMware Workstation Pro and find for the Windows 2008 victim machine. Once the Windows 2008 victim machine has been found, click the “power on this virtual machine” button to open the Window 2008 victim machine.

A screenshot of a computer

Description automatically generated

Figure : Enter password to login Window 2008

Once the Window 2008 has been powered on, a password is required before login to the Windows 2008 victim machine. A password of “p@ssw0rd” has been key in.

A screenshot of a computer

Description automatically generated

Figure : Press command prompt

Once login to the Windows 2008, click the window start button and press the command prompt to type in a comment to find the IP address of the Windows 2008 victim machine.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Figure : Find Windows 2008 victim machine’s IP address.

In the command prompt, key in the command “ipconfig” to find the IP address of the Windows 2008 victim machine. Once press enter, the IP address of the Windows 2008 victim machine will be shown.

A picture containing text, screenshot, computer, operating system

Description automatically generated

Figure : Key in username and password to login to Nessus

When the IP address of the Windows 2008 victim machine has been obtained, open the Nessus by typing the website link. The Nessus link is <https://localhost:8834/#/>. Then, key in the username and password before signing into the Nessus website.

A screenshot of a computer

Description automatically generated with medium confidence

Figure : Press “New Scan” button

Once successfully login to the Nessus, the GUI of the Nessus will be shown. “New Scan” button need to be clicked to add new scan for scanning the vulnerability of the Windows 2008 victim machine.

A screenshot of a computer

Description automatically generated

Figure : Press “Advanced Scan”

After pressing the “New Scan” button, a selection of vulnerabilities scan will be shown. Advanced Scan will be selected to scan the vulnerabilities of the Windows 2008 victim machine.

A screenshot of a computer

Description automatically generated

Figure : Fill in scanning details

Once pressing the “Advanced Scan”, some details will be needed to fill in, such as name and targets. The IP address of the Windows 2008 victim machine, which is 192.168.79.132 will key in at the Targets section.

A screenshot of a computer

Description automatically generated

Figure : Fill in the username and password

After filling in the name and targets section, press the credentials and choose the Windows section. The username, “administrator” and password, “p@ssw0rd” will be key in. Once done filling in the username and password, press the save button.

A screenshot of a computer

Description automatically generated

Figure : Press Play Button

After pressing the save button, a scan session will be shown. Click the play button to start scanning for the vulnerability of the Windows 2008 victim machine.

A screenshot of a computer

Description automatically generated with medium confidence

Figure : Result of the vulnerability scan

Once the scan session has been completed, press the scan session and the result of the scan will be shown. The total number of the vulnerabilities and the severity level of the vulnerabilities that present in Windows 2008 victim machine will be viewed.

# VULNERABILITY IDENTIFICATION

## Vulnerability 1: SSL Version 2 and 3 Protocol Detection (Sin Lian Feng TP065298)

### A screenshot of a computer error Description automatically generated with low confidenceIdentification

Figure : SSL Version 2 and 3 Protocol Detection Vulnerability

Based on the vulnerability scanning result, one of the critical vulnerabilities identified in the Windows 2008 victim machine is the detection of SSL Version 2 and 3 Protocol. In 1995, Netscape Communications Corporation introduced the Secure Sockets Layer (SSL) Protocol, a security protocol that protects data sent between a client's web browser and a server during transmission (Secure Sockets Layer (SSL) Protocol, 2023). This protocol ensures the data transferred between them remains private and free from cyberattacks. The SSL protocol stack has 4 layers, the first layer consists of Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol, and Hypertext Transfer Protocol (HTTP). Whereas the remaining layer consists of SSL Record Protocol, Transmission Control Protocol (TCP), and Internet Protocol (IP) respectively.

![A picture containing text, screenshot, line, font

Description automatically generated](data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEAYABgAAD/4RD6RXhpZgAATU0AKgAAAAgABAE7AAIAAAAQAAAISodpAAQAAAABAAAIWpydAAEAAAAgAAAQ0uocAAcAAAgMAAAAPgAAAAAc6gAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEFiaGlzaGVrIFRpd2FyaQAABZADAAIAAAAUAAAQqJAEAAIAAAAUAAAQvJKRAAIAAAADMDgAAJKSAAIAAAADMDgAAOocAAcAAAgMAAAInAAAAAAc6gAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADIwMTk6MDY6MTAgMTY6MTE6MTYAMjAxOTowNjoxMCAxNjoxMToxNgAAAEEAYgBoAGkAcwBoAGUAawAgAFQAaQB3AGEAcgBpAAAA/+ELImh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC8APD94cGFja2V0IGJlZ2luPSfvu78nIGlkPSdXNU0wTXBDZWhpSHpyZVN6TlRjemtjOWQnPz4NCjx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM6bWV0YS8iPjxyZGY6UkRGIHhtbG5zOnJkZj0iaHR0cDovL3d3dy53My5vcmcvMTk5OS8wMi8yMi1yZGYtc3ludGF4LW5zIyI+PHJkZjpEZXNjcmlwdGlvbiByZGY6YWJvdXQ9InV1aWQ6ZmFmNWJkZDUtYmEzZC0xMWRhLWFkMzEtZDMzZDc1MTgyZjFiIiB4bWxuczpkYz0iaHR0cDovL3B1cmwub3JnL2RjL2VsZW1lbnRzLzEuMS8iLz48cmRmOkRlc2NyaXB0aW9uIHJkZjphYm91dD0idXVpZDpmYWY1YmRkNS1iYTNkLTExZGEtYWQzMS1kMzNkNzUxODJmMWIiIHhtbG5zOnhtcD0iaHR0cDovL25zLmFkb2JlLmNvbS94YXAvMS4wLyI+PHhtcDpDcmVhdGVEYXRlPjIwMTktMDYtMTBUMTY6MTE6MTYuMDc3PC94bXA6Q3JlYXRlRGF0ZT48L3JkZjpEZXNjcmlwdGlvbj48cmRmOkRlc2NyaXB0aW9uIHJkZjphYm91dD0idXVpZDpmYWY1YmRkNS1iYTNkLTExZGEtYWQzMS1kMzNkNzUxODJmMWIiIHhtbG5zOmRjPSJodHRwOi8vcHVybC5vcmcvZGMvZWxlbWVudHMvMS4xLyI+PGRjOmNyZWF0b3I+PHJkZjpTZXEgeG1sbnM6cmRmPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5LzAyLzIyLXJkZi1zeW50YXgtbnMjIj48cmRmOmxpPkFiaGlzaGVrIFRpd2FyaTwvcmRmOmxpPjwvcmRmOlNlcT4NCgkJCTwvZGM6Y3JlYXRvcj48L3JkZjpEZXNjcmlwdGlvbj48L3JkZjpSREY+PC94OnhtcG1ldGE+DQogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAKICAgICAgICAgICAgICAgICAgICAgICAgICAgIDw/eHBhY2tldCBlbmQ9J3cnPz7/2wBDAAcFBQYFBAcGBQYIBwcIChELCgkJChUPEAwRGBUaGRgVGBcbHichGx0lHRcYIi4iJSgpKywrGiAvMy8qMicqKyr/2wBDAQcICAoJChQLCxQqHBgcKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKir/wAARCAGkAx4DASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD6Roor59svjn4/8S3V5J4P8GQ31jBLsDeVI7L6biGAzx6UAfQVFeFf8LN+Mn/RO4//AAFm/wDi6P8AhZvxk/6J3H/4Czf/ABdAHutFeFf8LN+Mn/RO4/8AwFm/+Lo/4Wb8ZP8Aoncf/gLN/wDF0Ae60V4V/wALN+Mn/RO4/wDwFm/+Lo/4Wb8ZP+idx/8AgLN/8XQB7rRXhX/CzfjJ/wBE7j/8BZv/AIuj/hZvxk/6J3H/AOAs3/xdAHutFeFf8LN+Mn/RO4//AAFm/wDi6P8AhZvxk/6J3H/4Czf/ABdAHutFeFf8LN+Mn/RO4/8AwFm/+Lo/4Wb8ZP8Aoncf/gLN/wDF0Ae60V4V/wALN+Mn/RO4/wDwFm/+Lo/4Wb8ZP+idx/8AgLN/8XQB7rRXhX/CzfjJ/wBE7j/8BZv/AIuj/hZvxk/6J3H/AOAs3/xdAHutFeFf8LN+Mn/RO4//AAFm/wDi6P8AhZvxk/6J3H/4Czf/ABdAHutFeFf8LN+Mn/RO4/8AwFm/+Lo/4Wb8ZP8Aoncf/gLN/wDF0Ae60V87X/xy+Jel6ta6XqHg2zt768x9nt5IJQ8uTjgb+ea1P+Fm/GT/AKJ3H/4Czf8AxdAHutFeFf8ACzfjJ/0TuP8A8BZv/i6P+Fm/GT/oncf/AICzf/F0Ae60V4V/ws34yf8ARO4//AWb/wCLo/4Wb8ZP+idx/wDgLN/8XQB7rRXhX/CzfjJ/0TuP/wABZv8A4uj/AIWb8ZP+idx/+As3/wAXQB7rRXhX/CzfjJ/0TuP/AMBZv/i6P+Fm/GT/AKJ3H/4Czf8AxdAHutFeFf8ACzfjJ/0TuP8A8BZv/i6P+Fm/GT/oncf/AICzf/F0Ae60V4V/ws34yf8ARO4//AWb/wCLo/4Wb8ZP+idx/wDgLN/8XQB7rRXhX/CzfjJ/0TuP/wABZv8A4uj/AIWb8ZP+idx/+As3/wAXQB7rRXhX/CzfjJ/0TuP/AMBZv/i6P+Fm/GT/AKJ3H/4Czf8AxdAHutFeFf8ACzfjJ/0TuP8A8BZv/i6P+Fm/GT/oncf/AICzf/F0Ae60V4V/ws34yf8ARO4//AWb/wCLo/4Wb8ZP+idx/wDgLN/8XQB7rRXhX/CzfjJ/0TuP/wABZv8A4uj/AIWb8ZP+idx/+As3/wAXQB7rRXhX/CzfjJ/0TuP/AMBZv/i6P+Fm/GT/AKJ3H/4Czf8AxdAHutFeFf8ACzfjJ/0TuP8A8BZv/i6y9c+OHxN8NW0Vxrvgq1sYppPLjeaCVQzeg+egD6JorweL4o/GGaFJYvh7EyOoZWFtNgg9D9+n/wDCzfjJ/wBE7j/8BZv/AIugD3WivCv+Fm/GT/oncf8A4Czf/F0f8LN+Mn/RO4//AAFm/wDi6APdaK8K/wCFm/GT/oncf/gLN/8AF0f8LN+Mn/RO4/8AwFm/+LoA91orwr/hZvxk/wCidx/+As3/AMXR/wALN+Mn/RO4/wDwFm/+LoA91orwr/hZvxk/6J3H/wCAs3/xdH/CzfjJ/wBE7j/8BZv/AIugD3WivCv+Fm/GT/oncf8A4Czf/F0f8LN+Mn/RO4//AAFm/wDi6APdaK8K/wCFm/GT/oncf/gLN/8AF0f8LN+Mn/RO4/8AwFm/+LoA91orwr/hZvxk/wCidx/+As3/AMXR/wALN+Mn/RO4/wDwFm/+LoA91orwr/hZvxk/6J3H/wCAs3/xdH/CzfjJ/wBE7j/8BZv/AIugD3WivCv+Fm/GT/oncf8A4Czf/F0f8LN+Mn/RO4//AAFm/wDi6APdaK8K/wCFm/GT/oncf/gLN/8AF0f8LN+Mn/RO4/8AwFm/+LoA91orwr/hZvxk/wCidx/+As3/AMXVZ/i58WY7xbSTwHbrcOMrEbeXcfw30Ae/UV4V/wALN+Mn/RO4/wDwFm/+Lo/4Wb8ZP+idx/8AgLN/8XQB7rRXhX/CzfjJ/wBE7j/8BZv/AIuj/hZvxk/6J3H/AOAs3/xdAHutFeFf8LN+Mn/RO4//AAFm/wDi6P8AhZvxk/6J3H/4Czf/ABdAHutFeFf8LN+Mn/RO4/8AwFm/+Lo/4Wb8ZP8Aoncf/gLN/wDF0Ae60V4V/wALN+Mn/RO4/wDwFm/+Lo/4Wb8ZP+idx/8AgLN/8XQB7rRXhX/CzfjJ/wBE7j/8BZv/AIuj/hZvxk/6J3H/AOAs3/xdAHutFeFf8LN+Mn/RO4//AAFm/wDi6P8AhZvxk/6J3H/4Czf/ABdAHutFeFf8LN+Mn/RO4/8AwFm/+Lo/4Wb8ZP8Aoncf/gLN/wDF0Ae60V4V/wALN+Mn/RO4/wDwFm/+Lo/4Wb8ZP+idx/8AgLN/8XQB7rRXhX/CzfjJ/wBE7j/8BZv/AIuj/hZvxk/6J3H/AOAs3/xdAHutFeFf8LN+Mn/RO4//AAFm/wDi6P8AhZvxk/6J3H/4Czf/ABdAHutFeFf8LN+Mn/RO4/8AwFm/+Lo/4Wb8ZP8Aoncf/gLN/wDF0Ae60V518IfiXd/EXTdSOqafHZXunSrHKsWQp3bscEkgjae9ei0AFeE/su/8i/r/AP19p/Jq92rwn9l3/kX9f/6+0/k1AHu1FFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFAHhXxX/5OE8B/SP8A9HGvda8K+K//ACcJ4D+kf/o417rQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAV4n+07/AMibon/YUT/0E17ZXif7Tv8AyJuif9hRP/QTQB69on/IA0//AK9Y/wD0EVeqjon/ACANP/69Y/8A0EVeoAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACvB/FzEftZ+HACcfZY+M+7V7xXg3i7/k7Xw5/16R/zagD3miiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKAPCv2bP+Pvxn/wBfsX85a91rwr9mz/j78Z/9fsX85a91oAK8J/Zd/wCRf1//AK+0/k1e7V4T+y7/AMi/r/8A19p/JqAPdqKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKAPCviv/AMnCeA/pH/6ONe614V8V/wDk4TwH9I//AEca91oAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAK8T/AGnf+RN0T/sKJ/6Ca9srxP8Aad/5E3RP+won/oJoA9e0T/kAaf8A9esf/oIq9VHRP+QBp/8A16x/+gir1ABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAV4N4u/5O18Of9ekf82r3mvBvF3/J2vhz/r0j/m1AHvNFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAeFfs2f8ffjP/r9i/nLXuteFfs2f8ffjP8A6/Yv5y17rQAV4T+y7/yL+v8A/X2n8mr3avCf2Xf+Rf1//r7T+TUAe7Vx/wATtVvdH8Irc6ZcNbzG6iTeoGcHORzXYVwXxkXf4DCgld15EMjt1rKs2qbaMa7apSaO6ibdChJySozXGeDdYv8AUPF/ia2vblpYLWdVhRgMINoPFMi+Ht0YUP8AwlmsjKjjzj/jWB4Eig0fVPGceoXk0kFu4825dvnK7Rk59azlKXNG6t/wxlKc+eN1b5+R2l58QfC9heG1udYt1lU4YBwQp9/StWfXNMttLTUpr2FbJyoWcsNp3HA59zXmemXUsnhOW38LeDt+lSRMVur6VVMgx944yT61iSbpv2dPJkOAL5UG0/dH2jtU+3lr6XI+sSSfo31/pnqiePfDL6kLFdYtjOx2gbxgn0z61q6rrGn6JZm61W6jtoQcbpGxk+lcP460HTLP4Wt9ms4ozbpG8bKuCrcc1VuY11j4i+GLPVB5ttHp/npG/KySbevuRVupNOz30/Et1ZxfK7X0/Eu6t42g1LxJ4Xj8Oaoslvc3jx3SRkHcAFwD6da6fWPGOg6BcC31XUoYJiM+WW+bHriuU8YaRYWnxE8JXttCkVxLdFHKjG4Dbj+ZqvqOma9oni/VdW0TTrPX7e8YGWEygSw9fl9h7VHPOLfr+hPPUi5ev6djpvEviGKb4falq3h++STZbu0U8JDYYA1R0L4haHFounQ6xrMAvpIVMu9gCGPr6VzKahpFz8O/FcOm6fNpl2qSPd2kv8Lleox2rX07w5pS/BpU+xRHfZF2YryW9c+tHPNyvHsJVJyleLW36neXWpWdjYG9u7mOG2VdxldsLj61jad498NarfrZ2WqwSTucIm7759vWuGN7pJ+F/hhNcgub+djH9ltIG5lcDgNngiqXja41a4s9MnvfDcGkRQ3kYil80GUc9AAMY/GnKs0rocsRJK68v68jtp9Wvl+Llvpi3DCyawaQw4GC2V5/U10dvrem3epzadbXkUt3AMyxK2Sn1ry/x1LrafEmIeGole9fS3XcxxsX5ST9eMfjWv4TurG1+FepXuiIyalFbzPdb+ZftCqc7j9Rx7YojUfO4hCs1OUfX+kdPf8Ajvw1pt+bK81a3jnU4ZS4+U+/pW7BPFcwJNbyLJE4DK6nII9a8d8GHWx4MiFr4QtL6K8UvLcyXADSk9SRiuw+F9jqOm6Bc2mpJHGiXLGCKOUSCNSSduR6dKqnVlJq63KpVpTaut/U7aiiiug6zwr4r/8AJwngP6R/+jjXuteFfFf/AJOE8B/SP/0ca91oAK4jxd4i1SXxFaeFvDDpFf3MZlmuXXcII84yB68Gu3rziPFh8eZPtR2i8sAYGPQ4LZH1rKq3ZJdWYVm7JLqx994S8V6TZtqGk+KLq8vIRva3nRSk2OqgAAil8S+J9Vj8K6BqG2XSri5vIkuYnXBA3AMDnsefwNd9dXMVnaS3NwwSKJC7MewFeZ/ELUbDxZ4R0We0LPZ3Woxx5ZcZG8KayqRUIvlZlViqcXyvpsdhZeOvDd7qC2Fvq1u9y3yhQ4+Y+grQ1fXtL0G3E2r3sVqjHC+Y2Nx9q4b4oaRYaf4HspbK1jgkt7uEROi4K9c1P4pvtOHjKw8jSLjWtcit9yQKwEcSnucng1TqSjdPy/Ep1Zxuna+n4nVaL4u0PxBK0Wk6jDcSoMtGrfMB64pl94z8P6b54vNUt42gk8qRS4yremPXivPopdRb4v6LPqOkW+lSywuuyKXczrn+LitTwVo9jeePvGN7d26TTR32yMuudoO7P8hSVWT0XcmNactFve34XO60nW9O12z+1aTdxXUOcFo2zg+hrNm8eeGbfUjYzavbLOpwwLjAPoT61wEMj6LrXxCi0hPJWG182NI+ArGMEsK6bwp4f0eb4XwJJawypc2xkmdlBLsc5JPrRGpOWi3HGtOeitfX8HY62z1nTtQ0976zu4pbVCwaVWyo29efbFZdn488NX+oCytdXt5J2baqhx8x9B615Ak81p8FbG0scyQ3GrNC43YDp5pwCfQ4FdHrtjr2o+FDp3/CH2VnHHGPJuBdAeUQOG6VHt5NaLoZ/WZNaLpfqeu1xfjHxFqY1yy8MeGWSPUbxTI9w43CCMZycevBro/D32r/AIR2w/tFg115C+aQ2QWxzz3rjJSLD47RPdnat7Y4gZumQDkfXitqknyq3U3qyfKraXaFvPCHizTbNr/S/FN1d30Y3tBMimOX/ZwAMVo3GrXupeD9Nvb68bw3dSTRiUTJjcdwBUA9m7fWuunnjtreSedgkcalmY9gK828da7ZeI/BemahpjM9u+pQhSy4ziQComlTTs/kROMaSbT6bXO3v/E2jaPJ5Op6lBBKsIlKu4BK8jOPwNLovibR/EKudIvorkx/fVG5X6iuKvtNs9R+OGnfbkWTydIV40bkFt78/hUniSGPS/i54Zn01FimvhLFchOPMQDIz9CBT9pLfpew/azV30vYi8MePILK78Qf8JPqyqkOotFbrIQCFAHArvtL1iw1qxF5pd1HcwE43xtkA+leefDXSLG68ReKry5to5Z11F41Z1zheD/Ws+CWTQ4viOmkjyltijQxpwEJznFRCpKMU3tqZ06s4xTlqtfXS531z4+8MWmoGyn1i2WZW2sN4wp9Ca1bzV7DT7OO6vLuKKCVgqSM2AxPTBryrw3DrI8C29pbeDbO5tbm2DPO1yMy7hkueOveqWu2N/b/AActrHV9oZNSRIxHIH2oWyBkemTR7aVr26B9YnyttdL9T1rSPE2j67PPDpN/FcvAfnEbZxWrWfpWjadpFuq6bZw2wKAHy1xnFaFdMb2947I81ve3CvE/2nf+RN0T/sKJ/wCgmvbK8T/ad/5E3RP+won/AKCaoo9e0T/kAaf/ANesf/oIq9VHRP8AkAaf/wBesf8A6CKvUAFFNllSCF5ZWCoilmY9gK5Twd4/tPF17d20VvJbSQAMgk/5aoSRuHtxUuSTSfUhzipKLerOtorD17xLHoepaXaPA0h1CfyVYH7vBOf0rcpppuw1JNtLoFFFFMoKKzNL16z1i8vrezLlrGTypSRgbvarWo3g0/S7q9Zdwt4XlKjvtUnH6Urpq5PMmros0V5zY/EzV9Ssoryx8IXs1vKMpIrrhh09a6Hwt41tPEs9xaG3nsb+1/1trcKAwHqME5FZxqwk7IzjWhJ2TOlooorU2Ciq9/ew6bp895dErDAhdyB2AzTdM1CHVtMgvrYMIp13JuHOKV1ewrq9i1RRRTGFFFFABRWb4h1hdA8P3mqSRmVbWIyFAeTip9Lvhqek216qlBcRiQKe2aV1exPMr8vUt14N4u/5O18Of9ekf82r3mvBvF3/ACdr4c/69I/5tTKPeaKKKACiiigAooooAKKKKACisPTvEseoeLNV0NYWV9OVGaQnhtyg/wBad4q8RJ4Y0Q6jLC0yiRY9qn1qeeNrkc8eVy6I2qK5PW/Fuq6bdpHp/hy61CJ4w/mxMoAyOnJrBsPinqeqCY6f4TvJxBIYpNrr8rDqOvvUOtBOzIdeEXZ/kz0qiuIvfG+t2giKeEr2VWhWRyrr8hIyVPPaszTvinqerQvLp3hO8uEjcxsyuvDDqOtL20E7foJ4imnb9GelUVxGufEG50nVrPTbfQ7i8vLmDzvKRgCo7jk1Vf4m3OnFZfEHhm/sLQsFaf5WCZ4ycHpTdaCdgdemnZs9BoqO3njuraOeBg8cihlYdwakrU3CiiigAooooAKKKKAPCv2bP+Pvxn/1+xfzlr3WvCv2bP8Aj78Z/wDX7F/OWvdaACvCf2Xf+Rf1/wD6+0/k1e7V4T+y7/yL+v8A/X2n8moA92rD8W+G08VaKNPknaACZJdyj+72rcopNKSsyZRUlZiIuyNV9BiuXtPA9tDca81xO00Wtf61Om0YxgV1NBIAyTgDuaTinuEoRlucFZeAdZtdLXRj4nnGkovlrEkSCTZ/d3balX4bQp4Efwyt8/kfaRMkmBlQH34rs/tVv/z3j/77FSKwYZUgj1BqPZQMlRp/oZHiDw+uu+GZNIeZoldFXeByMVna74Kj1az05ra8kstR01QLe7jxkYGMEdwa6miqcIvcuVOMt0cNB4Avp/EGna1rmvTX13YyblXYqpj0AAH51Pf+CtQi1671TwzrcmmSXpzcRGNXRm9QCDg12VFT7KNifYwscba/D2KLQNWtLm/lub7VlIubtwMnIxwAMYFbcGgrD4SXQxMSqweT5mOfrWvRVKnFbFRpwjsjiLv4cRzeHNJsbbUJLe80khre6UAnIGORjGKr6p8OtR8QwRnX/EU9xNA4eHy0VEQjvgDkn3rv6Kl0YPoS6FN9DBbwwjeModfM7b47Y2/lY4OSOf0qCz8Gwaf4qvdUtJiltqCYurPHyO2MbsetdIzBVJYgAdSTSgggEHIPQ1XJEr2ce3mcEngDVtME1p4d8STWWmzMWNu0auY89QpIJFdN4Z8OWvhjRksLNnkAJZ5ZDlpGPJJNa9FKNOMXdCjShF3QUUUVoanhXxX/AOThPAf0j/8ARxr3WvCviv8A8nCeA/pH/wCjjXutABXP+KvCFp4pt4TJLLaXls26C6gOHjP1roKKUoqSsyZRUlZnn0/w/wBe1WNbPX/Flxc6eCN0McaoXHoSACa3dY8G2mo6Vpmn2zfZINPnjljVB12kHH6V0Mk0cQzLIqD/AGmApY5Y5VzE6uPVTms1TgtDNUYK67mJ4r8NJ4o0NdOknaELKku9R/d7Vm614LubnxDFrmh6q+nX6xCGQ7A6yKPUEH0rr6KqVOMtypU4yd2cVbeAJl8TWOv3+sz3l/bkiQuoCsv90AAAd/zra0Lw4miatrF6k7SHVLgTspH3OvH61t0UlTindBGlCLukcunhmDSdX1/XZC92uoQjzLYLnIVQMD1ziuAt10RfDs72PjSex0tgxbTGkTzEP9wZG4fSvZ6yn8MaJLd/apNMt2mzneU71E6V/hMqlG/w/wBXOK8B+EINT+EUOl6tDJEly7zJ2aMF9yMD69Kty/D7Wb+0j0zV/FFxcaVGQPJWNVd1HZmAya7sywQ4QyRx4HClgMUqTRSHEciMf9lgaaowskxqhDlUX0VhLeCO1t44IFCRxqFVR2ArE8VeEbPxVaRLPJJbXNu2+C6hOHjPsa36K0cU1Zm0oqS5XsefzeAPEGpQrZa14tubjThw0Ucaozj0LBcmtrV/BVlf+H7HSLNvsdvZTRyIEH9wg4/SumoqVSgjNUYJPzPLPEekXGp/Giyhsb+SxuYdIDRTxgHBDvwQRgiuo0PwZNaa4db1/UpNV1FUMcTsoVYl77QAOeK6U2kBvBdGJfPC7BJjnHpU1TGkk233FGjFScn3uc/4Z8LJ4cudUmS4ab+0Lo3BBH3Mjp+lNsPCNvaarrt1NIZ01llMkTDhQARj9a6Kir5Iq3kWqcUkrbHAR/D7WLC0k0zR/FFxbaS+QIGjVnRT1VWIzitC/wDh9ZXPhC00C2nkhit5lm8w8s7A5JOfWuvpA6sxVWBZeoB5FT7KC0JVGmlawKNqgegxS0UVqbBXif7Tv/Im6J/2FE/9BNe2V4n+07/yJuif9hRP/QTQB69on/IA0/8A69Y//QRV6qOif8gDT/8Ar1j/APQRV6gDifirrf8AZfg9rSKZYrjUnFrGztgANwxz7A1yOoXmieFNe8M6noupWkyRRixu0hnVmKHBBwD655rqNV0C68TfEyBtVsGbRdOt8oZB8k0jA8j6Z/SrviL4faJqHh+8trHTYILl4z5UiLyrdsVyTjObcl8vkcM4VJylKPTb5Gf8QSG8TeEipyDfZBHf5GrF1zxVHrXje/0i/wDEX9habp21f3bqjzuRk8nsOKkh07xHqeneDm1HS7iO50+523O4D5VVSoY89+Pzqe+0W68M+OdR1U6GdZ0zU9rsIlDPA4GOh7HiolzPVbNr8iJOUryWibV/uG+E/FfkeKLrw9DrY1qya2aa2uSys6MOqkjr1/Sq3hDS/EHi+GW/vfEV5aw215JHFHDgb1DnO7j8K3fDsWqajrV5fNosWk6YICkEUkYE0jn+LI6D2q98N9LvdJ8OzwajbPbytdzOFfqVLkg/lVRi5NJ7alQg5NKW2vc5v4Z6JJD4m16c6ndSC3uyhjYjbLx95uOtd/4m/wCRT1f/AK8Zv/RZrkvCcWq6J421qzutJnNrfXPnRXi/cxjvXYa/BJc+G9TggQvLLaSoiDqzFCAK0pK1Nr1NaKtSaXmeZ+BviAdL8D6ZZDw9q1z5MRHmw27Mj/MTwcVoaDaarqfivWvGN5p82lRvp7W9vBMNshxzuI/Cuo+H+nXOmeAtKs9Qt2guYYiJI3HKncTW5qMbS6XdRxqWd4XVQO5KmlCnJxjzPYmnSk4Rcnt0+R5f4Jg1vWdHg8Tatr9ysFo7stvHjbIiMc7uOehq3oWl6147sJNcvtevLBZXYWkFoQqoo6E8c1t/D3RLqz+HsemavbvbSuZleN+oDO39DWP4fv8AXfBGnyaHd6DdagkMjG1uLXBV1PQHPTFZxjZR5r2t+JnGNox572trvuUZr7U9b8D+I9I1i9kW80YujTxAD7QgBxnjuKLa+1Dwt8MdKj0u+lnv9WdYrdpwCIc8cDHb3rS0fwtq7+F/Et1qUSx6lrQkkW2Bz5Ywdq59elZ66RreufD+xt00uWx1XRJFeFZ/uzFTnj60rS362/X/ACJtPfW9v1/Oxb1nw9rnhXRX16x8R3t3c2oEk8FxtMcq55AGOOtT6v4g1HxLqmhaJo102nrqVmLy5uI1BZFwflGe/FRa3rfiHxVoT6FZ+G7uzuLoCO4muCBHCueSCOvSpdW8Paj4c1bQdb0S0bUBp1oLO4t0OGdMYLD356VT/u3toU+vJfl0vv8AMvWWh694X1hZoNVm1LR2iZrhbtwXjYcgg9fWsfw9Yav8QdOk1+81280+GaRxaW9qQoRQSATxzWpDqHiHxVr0CxWFxpOjxRuLj7SAGnYjAUD0HNZvhy61vwDp8ug3GhXWowQyObO4tsESKSSA2elHu3W/KP3brfl17+RRu9d1C7+H/i7RNakE97pMbRmcDHmIVypOO/NeheE/+RQ0v/r2T+VcKnhTWZfBnim+vbU/2trasy2sfJVQuFX613/hu3ltPDOn29zGY5Y7dVdG6qcdKukpc132/Uugpc15dv1NOvBvF3/J2vhz/r0j/m1e814N4u/5O18Of9ekf82rpOw95ooooAKKKKACiiigAooooA8mGp61p3xe8TnQtJXUWdIBIDIF2/u096q/EHXfFF74X8nVvDy2VsbiMmYTBsHPpmux0HSr62+KHiXUJ7Z0tLpIRDMR8r4RQcfiDUnxL0y91fwe1rptu9zP9ojbYg5wCcmuNwk6ctX1PPlTk6UtX10+Z09l/wAeEH/XNf5Vwnwn/wBT4h/7Csn/AKCtd5aKyWcKuMMqAEenFch8N9Iv9Jj1sajayW5n1GSWLePvqQuCPyraSfPH5nTJP2kPmdhdf8ec3/XNv5VwXwe/5F/U/wDsIzf+hGu+uFL2sqqMkoQB68Vxvww0i/0fRb+LU7WS2kkvpJEVx1Ung0ST9pF+oST9rF+pgeMNY/sP4xadeCzuLzFiy+VbIWc5I5wKk8SeKtS8X6HPoek+FtSSW8whluoSkcYyOSSBW1f6Pfy/F+w1NLR2sY7Jo3nx8obI4rtwAOgxUKEpOSvZXMo05yc1eybM/QdPbStAsrGRtzwQqjH371oUUV0JWVjrSsrIKKKKYwooooAKKKKAPCv2bP8Aj78Z/wDX7F/OWvda8K/Zs/4+/Gf/AF+xfzlr3WgArwn9l3/kX9f/AOvtP5NXu1eE/su/8i/r/wD19p/JqAPdqKKKACsnxUzJ4S1NkJVhbOQR24rWrH8Wf8ihqn/Xs/8AKpl8LIn8LOA8FfDnRtc8H6fqV/LfNcTxB3ZbtwM/QGrXhS4n8N+PtX0BL+e/0yC3E6iWQu0BxkjJqh4I+HNtq/g3T72TXdYtzNEGMUFwqovsBtrtNO8H6X4W0XUDp6ySTzRMZbid90j8dzXJTg7RaVjipU3aMlG3n3KWnfE/S9V1K2tNPs76cTttaZISY4j6M3QdKfffEnTre+nt7CwvtTFsxWaW0hLIhHUZ7/hWd8N4NnwtlNsirK7TNkDknFT/AAga2Hw9t1XaJlkkFwG+9v3HOauMpysr76lwnUlypvdXLHiHxtbS/Dq81nQnlmJjZFaJTuhfH8Q6jFN8I+MbcfD231LWjPAttAglmuFOZmI6r3bNcnZbW0T4iPZf8eBLiLb93dsG7FLrxz8L/BTS82az2/n+mNpxn2zUe0lfm8v1I9rO/P5frY6y3+J+mtPD9usNQsLadgsV1cwFY2z057Z962vEPivTvDlrDJds8slwcQQQqXeU+wFZfxJksB8N9SNwYzEYMQ4x97HyY/HFcnpgkj+Inhb+2c7TpREPmf8APXI/XGK0lOcXy37Gkqk4PkvfbX1O00Px1Y6zqh02a1utOvSu9IbuPaZB6g9DVS9+JWnQX09tp9jfan9nO2aS0hLIh7jPc/Srfia80eHUYIJow+szW8osmVcsp2NnpWb8J3tf+EHUIUFws8guvXfuOc/hinzT5uS5XNPm5L/Md4n8Q2eu/CrVdR0iclfJweqsjbhwR1BrpfDbFvCuksxJJsoSSe/yCvKn2NofxHay/wCPIzr5e37pbcc4r1Twz/yKekf9eMP/AKLFFOTlK77fqxUZuc7vt+rNOiiiug6wooooA8K+K/8AycJ4D+kf/o417rXhXxX/AOThPAf0j/8ARxr3WgAoooPSgDySWPTfE/xE1qx8aajJbx2kgSytGnMMbpz8/UAnp+db+leELjw74ntLnwrdySaNKpW6tpLgyKvoy5NPjPhjx/fX9lq2lxpfafKYmWR8Sf7wIxxWBfaT/wAID4y0NfD2p3MsOpXQhnsZpN4CE4LDuAP6VxWS97fXfqefZR99q6vv13Or1P4h6Zpus3Gki3urm/h2kQQRli4OeR9Md/Wr/hzxdYeI2nhhSa1u7f8A11rcJtdB647j3Fc14fa0Hxk8QibZ9pMEXlZ64y27H6VX1ffJ8Wbr+yj+9TSJPtHl+u35M/jitFUl8XnY0VWa95vraxs3vxJ06G+ntrCwvtTFuds0tpCWRD3Ge5+lblj4m0rUNAOs290v2NVLO7cbMdQQeQa80+H1j4nn8L7tG1rT7ePzpBNFLbFnV887juGTVSfTpLH4feJSmqQ6gkl7G9wLWMokXz/MAMnioVaduZkRr1LczW6Z2i/FPS9ySy2GoRae7bVv3gIiPPX1x7120UqTRLJEwZHGVYdxWBPcaJB4Djm1JYn0tbRGZcZBXaO3rWvpcttPpdvLYqUtmQGNSMYXtXRByvZu5003K9pO55lqOg23if416nYanLcfZ4rGORVimZMNhR2PvUXjXwzB4A0eLXPDmo3lvcxToPKkuWdZgT0IJ5pdT8Ox+JPjhqltLfXlkI7CJ99pIEY8KMEkHiulsvhZpFvfRXN7fajqZhbckd7OGQH1wAK5eRy5rLW71ONU3PmtHW71LOr/ABC03QriK0vobh7uW3EyQwxlmfp8oA78/pTp/iDplrodpf3FvdxzXhIhsjEfPYgkfd7dKyL23im+OVj5iBvL092TI6HKj+tF9sj+ONgb7aEawYW27pu+bOPetOeeuvWxs6lS7162NnRvH2n6rqQ064trrTr1l3RwXcZUyD/ZPQ1z+k+M7m5+LWp2MtvfG1EKRxRFDtiPGXI7A+vvU3xHMbeIPDCW206gb393t+9txz+HSpNOLf8AC4/E4jOJDp0O367VxScpcyjfZ/oKUp8yjfZ/oaOpfEXT7PUprGwsr3VJbfic2cRZYz6E9M/StbRfFOl67pMmoWc+2KHPnLICrREdQwPSuY+EjW48O365UXQv5ftGfvbs9/wrl9S8ySX4gnRf9QEQN5fTzN3zfpmn7WSSk+vQPbTUVN63vode/wAVNKXdOlhqEmno21r9bc+UPU+uPetnWfGek6Np1tdSStcG8H+jRQKXeb6AVBos2kJ8NrSSfyjpy6epmHbAT5v61x9lc6dcfFrQ7i2TZpMmlsLBXGAH3DpnvTc5pLXcbqTilqtbHW6L490/VdUGm3NtdabeON0cN5HtMg9j0NY/g6aV/iv40jeRmRHh2qTwvy9qi+KBRtX8LJaYN/8A2mhG373l87vwxTvBn/JW/G3+/B/6BScnzqL6P9GJyk6kYvo/0Z6JRRRXUdoV4n+07/yJuif9hRP/AEE17ZXif7Tv/Im6J/2FE/8AQTQB69on/IA0/wD69Y//AEEVeqjon/IA0/8A69Y//QRV6gAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAK8G8Xf8AJ2vhz/r0j/m1e814N4u/5O18Of8AXpH/ADagD3miiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKAPCv2bP+Pvxn/1+xfzlr3WvCv2bP+Pvxn/1+xfzlr3WgArwn9l3/kX9f/6+0/k1e7V4T+y7/wAi/r//AF9p/JqAPdqKKKACoL2zi1CxmtLkExTIUcA4yDU9FAblLSNKtdE0qDT7BWW3gXagY5IH1q1NEs8LxSco6lW+hp9FKySsJJJWRn6LotnoGmLYacjLArFgGbJyetYd98ONDvL6e6jN1ZtcnM6WsxjWQnrkCusoqXCLVmiXTg1ZoyrPw1pVhoL6PbWqpZOpV4/7+eufU1Q0zwHoml6LdaTHHLPZXON8U8m8LjpjPSukoo5I9g9nDscfbfDLQYbiF5Td3Udu26KC4nLxofZTWzr3hfTPEdpHBqUJPknMUkZ2vGfY9q16KFTglawlSglZI53RPBOlaHftfRefc3jLtE91IZGUegJ6VVvvhxol5fzXcZurN7g/vltZjGsn1ArrKKPZwtaweyha1jEj8I6PD4Zl0GC28uxlXDqhwW5zkn14rVtLWOysoLWAERQRrGgJzhVGB/KpqKpRS2KUYrZBRRRTKCiiigDwr4r/APJwngP6R/8Ao417rXhXxX/5OE8B/SP/ANHGvdaACiiigDmNe+H2heIb8X11FLDeAY8+3k2MfqR1o0H4f6H4f1A39tHLPeYwJ7mTzGX6E9K6eio9nC/NbUz9lDm5ranl8fhS3174o68+oR3EISOIwXERKMD82cN+Vdv4f8K6Z4bSX+z43Ms5zLNK293Pua2aKmNOMXfqTCjGDv1OSvfhtod3fT3UJurJ7g5mW1nMayfUCtjTvDWlaVoZ0iztEWzYEPGRnfnqT6mtWiqUIp3SKVOCd0jjY/hd4eR0Vvtclqj71tHnJhBzn7vTFdiiLHGqIAqqMADsKWinGEY7IcYRh8KMuLw9YQ+JZ9dRHF9PEIXbdwVGMcfhWpRRTSS2KSS2M19BsX8RJrbI321IjCG3cbSQen4CofEHhfTPE0EaanExaFt0UsbbXjPqD2rYopcsWrWE4Raaa3Ob0bwLpGjal/aEYnurzbtWe6kMjKPQE9KkvvBWk33iaPXpBPHfIFBeKUqHA6Bh36V0FFL2cbWsT7OFrWOV1L4eaLqGpS36G5sp5/8AXNaTGPzPrjrWto/hzTND0ptO0+2VLd87w3JfPUk961KKFCKd0hqnBO6RxjfC3w8zso+1ras+9rNZyISc5+70x7Vsax4R0fXNPgtLy22pbf6hojtaL/dPatuij2cErWEqUErJHN6N4F0jRtS/tBPPu7wLtWe6lMjIPbPStCw8PWGm63qGq2qOLrUSpnYtkHaMDA7VqUU1CK2Q1TitkFFFFUWFeJ/tO/8AIm6J/wBhRP8A0E17ZXif7Tv/ACJuif8AYUT/ANBNAHr2if8AIA0//r1j/wDQRV6qOif8gDT/APr1j/8AQRV6gAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAK8G8Xf8na+HP+vSP+bV7zXg3i7/k7Xw5/16R/zagD3miiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKAPCv2bP+Pvxn/wBfsX85a91rwr9mz/j78Z/9fsX85a91oAK8G/Zinhg8Pa+ZpUjBu0xvYDPDV7zXyt8IfhxbfEPwpqsF1qd1YC2vlYG3xlshutAH1D/aFn/z9wf9/R/jR/aFn/z9wf8Af0f414t/wzHpf/Q06t+Q/wAaP+GY9L/6GnVvyH+NAHtP9oWf/P3B/wB/R/jR/aFn/wA/cH/f0f414t/wzHpf/Q06t+Q/xo/4Zj0v/oadW/If40Ae0/2hZ/8AP3B/39H+NH9oWf8Az9wf9/R/jXi3/DMel/8AQ06t+Q/xo/4Zj0v/AKGnVvyH+NAHtP8AaFn/AM/cH/f0f40f2hZ/8/cH/f0f414t/wAMx6X/ANDTq35D/Gj/AIZj0v8A6GnVvyH+NAHtP9oWf/P3B/39H+NH9oWf/P3B/wB/R/jXi3/DMel/9DTq35D/ABo/4Zj0v/oadW/If40Ae0/2hZ/8/cH/AH9H+NH9oWf/AD9wf9/R/jXi3/DMel/9DTq35D/Gj/hmPS/+hp1b8h/jQB7T/aFn/wA/cH/f0f40f2hZ/wDP3B/39H+NeLf8Mx6X/wBDTq35D/Gj/hmPS/8AoadW/If40Ae0/wBoWf8Az9wf9/R/jR/aFn/z9wf9/R/jXi3/AAzHpf8A0NOrfkP8aP8AhmPS/wDoadW/If40Ae0/2hZ/8/cH/f0f40f2hZ/8/cH/AH9H+NeLf8Mx6X/0NOrfkP8AGj/hmPS/+hp1b8h/jQB7T/aFn/z9wf8Af0f40f2hZ/8AP3B/39H+NeLf8Mx6X/0NOrfkP8aP+GY9L/6GnVvyH+NAFb4q3MD/ALQHgV0njZFCbmDggfvj3r3L+0LP/n7g/wC/o/xrxJ/2XNGkkWR/Eups6/dYqpI/WpP+GY9L/wChp1b8h/jQB7T/AGhZ/wDP3B/39H+NH9oWf/P3B/39H+NeLf8ADMel/wDQ06t+Q/xo/wCGY9L/AOhp1b8h/jQB7T/aFn/z9wf9/R/jR/aFn/z9wf8Af0f414t/wzHpf/Q06t+Q/wAaP+GY9L/6GnVvyH+NAHtP9oWf/P3B/wB/R/jR/aFn/wA/cH/f0f414t/wzHpf/Q06t+Q/xo/4Zj0v/oadW/If40Ae0/2hZ/8AP3B/39H+NH9oWf8Az9wf9/R/jXi3/DMel/8AQ06t+Q/xo/4Zj0v/AKGnVvyH+NAHtP8AaFn/AM/cH/f0f40f2hZ/8/cH/f0f414t/wAMx6X/ANDTq35D/Gj/AIZj0v8A6GnVvyH+NAHtP9oWf/P3B/39H+NH9oWf/P3B/wB/R/jXi3/DMel/9DTq35D/ABo/4Zj0v/oadW/If40Ae0/2hZ/8/cH/AH9H+NH9oWf/AD9wf9/R/jXi3/DMel/9DTq35D/Gj/hmPS/+hp1b8h/jQB7T/aFn/wA/cH/f0f40f2hZ/wDP3B/39H+NeLf8Mx6X/wBDTq35D/Gj/hmPS/8AoadW/If40Ae0/wBoWf8Az9wf9/R/jR/aFn/z9wf9/R/jXi3/AAzHpf8A0NOrfkP8aP8AhmPS/wDoadW/If40Ae0/2hZ/8/cH/f0f40f2hZ/8/cH/AH9H+NeLf8Mx6X/0NOrfkP8AGj/hmPS/+hp1b8h/jQB7T/aFn/z9wf8Af0f40f2hZ/8AP3B/39H+NeLf8Mx6X/0NOrfkP8aP+GY9L/6GnVvyH+NAHtP9oWf/AD9wf9/R/jR/aFn/AM/cH/f0f414t/wzHpf/AENOrfkP8aP+GY9L/wChp1b8h/jQB7T/AGhZ/wDP3B/39H+NeLftMXVvN4O0UQzxyEaopIVwcfKaP+GY9L/6GnVvyH+NRzfsuaPOoWXxNqbAHI3Kp/rQB7Bot/ZjQdPBu4Afs0f/AC0H90Vd/tCz/wCfuD/v6P8AGvFR+zFpQAA8U6rgew/xpf8AhmPS/wDoadW/If40Ae0/2hZ/8/cH/f0f40f2hZ/8/cH/AH9H+NeLf8Mx6X/0NOrfkP8AGj/hmPS/+hp1b8h/jQB7T/aFn/z9wf8Af0f40f2hZ/8AP3B/39H+NeLf8Mx6X/0NOrfkP8aP+GY9L/6GnVvyH+NAHtP9oWf/AD9wf9/R/jR/aFn/AM/cH/f0f414t/wzHpf/AENOrfkP8aP+GY9L/wChp1b8h/jQB7T/AGhZ/wDP3B/39H+NH9oWf/P3B/39H+NeLf8ADMel/wDQ06t+Q/xo/wCGY9L/AOhp1b8h/jQB7T/aFn/z9wf9/R/jR/aFn/z9wf8Af0f414t/wzHpf/Q06t+Q/wAaP+GY9L/6GnVvyH+NAHtP9oWf/P3B/wB/R/jR/aFn/wA/cH/f0f414t/wzHpf/Q06t+Q/xo/4Zj0v/oadW/If40Ae0/2hZ/8AP3B/39H+NH9oWf8Az9wf9/R/jXi3/DMel/8AQ06t+Q/xo/4Zj0v/AKGnVvyH+NAHtP8AaFn/AM/cH/f0f40f2hZ/8/cH/f0f414t/wAMx6X/ANDTq35D/Gj/AIZj0v8A6GnVvyH+NAHtP9oWf/P3B/39H+NH9oWf/P3B/wB/R/jXi3/DMel/9DTq35D/ABo/4Zj0v/oadW/If40Ae0/2hZ/8/cH/AH9H+NH9oWf/AD9wf9/R/jXi3/DMel/9DTq35D/Gj/hmPS/+hp1b8h/jQB7T/aFn/wA/cH/f0f414T4tuYG/aw8OyrNGYxax5cOMDlu9Xf8AhmPS/wDoadW/If41E37LejtOJj4m1MuvRii5/PNAHt39oWf/AD9wf9/R/jR/aFn/AM/cH/f0f414t/wzHpf/AENOrfkP8aP+GY9L/wChp1b8h/jQB7T/AGhZ/wDP3B/39H+NH9oWf/P3B/39H+NeLf8ADMel/wDQ06t+Q/xo/wCGY9L/AOhp1b8h/jQB7T/aFn/z9wf9/R/jR/aFn/z9wf8Af0f414t/wzHpf/Q06t+Q/wAaP+GY9L/6GnVvyH+NAHtP9oWf/P3B/wB/R/jR/aFn/wA/cH/f0f414t/wzHpf/Q06t+Q/xo/4Zj0v/oadW/If40Ae0/2hZ/8AP3B/39H+NH9oWf8Az9wf9/R/jXi3/DMel/8AQ06t+Q/xo/4Zj0v/AKGnVvyH+NAHtP8AaFn/AM/cH/f0f40f2hZ/8/cH/f0f414t/wAMx6X/ANDTq35D/Gj/AIZj0v8A6GnVvyH+NAHtP9oWf/P3B/39H+NH9oWf/P3B/wB/R/jXi3/DMel/9DTq35D/ABo/4Zj0v/oadW/If40Ae0/2hZ/8/cH/AH9H+NH9oWf/AD9wf9/R/jXi3/DMel/9DTq35D/Gj/hmPS/+hp1b8h/jQB7T/aFn/wA/cH/f0f40f2hZ/wDP3B/39H+NeLf8Mx6X/wBDTq35D/Gj/hmPS/8AoadW/If40Ae0/wBoWf8Az9wf9/R/jR/aFn/z9wf9/R/jXi3/AAzHpf8A0NOrfkP8aP8AhmPS/wDoadW/If40Ae0/2hZ/8/cH/f0f40f2hZ/8/cH/AH9H+NeLf8Mx6X/0NOrfkP8AGj/hmPS/+hp1b8h/jQB7T/aFn/z9wf8Af0f40f2hZ/8AP3B/39H+NeLf8Mx6X/0NOrfkP8aP+GY9L/6GnVvyH+NAEX7NZzdeMyOR9ti/nLXu1eCfsxQC1/4S63ViwiuoUDHqceaK97oAK8J/Zd/5F/X/APr7T+TV7tXhP7Lv/Iv6/wD9fafyagD3aiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKAPCv2bP8Aj78Z/wDX7F/OWvda8K/Zs/4+/Gf/AF+xfzlr3WgArwn9l3/kX9f/AOvtP5NXu1eE/su/8i/r/wD19p/JqAPdqKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooA8K/Zs/4+/Gf/AF+xfzlr3WvCv2bP+Pvxn/1+xfzlr3WgArwn9l3/AJF/X/8Ar7T+TV7tXhP7Lv8AyL+v/wDX2n8moA92ooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigDwr9mz/j78Z/9fsX85a91rwr9mz/j78Z/9fsX85a91oAK8J/Zd/5F/X/+vtP5NXu1eE/su/8AIv6//wBfafyagD3aiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooA5jxh450/whFEtwklzeXHENrCMs3v8ASuUPxV1+3X7RfeDLqOzHJkV9zAeuKp/EFp/DPxO03xXeWT3mlxwCJiq58psk59utddpXxP8ACGuRiNNThiLjBjuf3efb5utcjm5TacrHC6kpVHFz5bbI2PDPijTfFekrfaVIWXO10YYaNvQisLxX8SbPw9qQ0qws5tT1RhnyIBwn+8e1XfCXgzTvDN5f32lXcssWouZTGSPLTJz8uK87l1X/AIV18WNW1LxDZSyWWpHMN4qFtg9Af6fSnOc4wXNp3ZVSpUhTjzaX3Zt/8Lb1TTmWTxH4TurG1JwZo237fc16HZavaanoyanp8gmt5I96MO/tXPw+M/CHi/TprBNUtmW6jMZjmIRjkY4Dd6teHvC9v4R8Kz6dZXU1zDlpFaYjK5HQY7VUHK+90VTc7/FzIj8C+M08aaXPeJam2EMvl7S2c11FeV/AX/kVb/8A6+j/AFr1Sroycqaky8PNzpRlLcK4Xxp8Rn8Ka9a6VBpUl/Ncxl1CNg/TFd1XkXji7t7H43eHLi9njt4EhctJKwVV4PUmprScY6O2qFiJyhC8XbVF4fFXWc/P4OvgPat3wl8SdM8UX76c0E9hqEYybe4XaWHtWq3jfwuqknxDphx6XSf415j9rt/F3x1sL7wyvmW9kpN1dRr8rfKR178ms3KUGrSvdmMpzptWnzXex7XRXGeNfG8+hX1po2h2Yv8AWb3/AFUR+6gzjLVi33iD4geF7X+1dbsrO8sFwbhIPvRD1GDzWsq0U2uxvKvGLa103PTaK5668Z6XbeCj4m8zdZmISKO5J6L9cnFclZa38R9fsf7W0yxsbS0cFoIJfvSL75PFOVWKdlqOVaKdlr6Hp1FcT4W+IcWr+H9Ru9YgFjd6Udt5F2U+2fpWLp3ijx14xjfUPDllaWWm7iIXuPvS4+ppe2jZW1uL6xCytrc9QorhPCHjy8v9en8OeJ7NbHWIF3DYfklX1FY2rfETxGPHGoeGtD06G5uFAFsTwF7ksemMZodaCjcTxEFFS+XzPVKR22Rs390E1wE3jPW/Cngua/8AGdpCNR84xW8EDZ8zgYPHuapDV/iTHpravdabZNbFC72anDqmO3Oc+1DrR7MHXitLP7tjpvBvjFPFw1LZbG3+w3TW5y2d2O9dPXlHwKuPtVhr9wFKedqLPtPUZAOK9Xp0ZOdNSY8PNzpKTPNde+LEuleKLrRbPQ5r6W3xkxN1Hriq4+MN5Eu+88J6jHGPvMqZwKqaBPFb/H7XGnlSNfs+Mu2PSvTLvWtJgtZHu7+1WIKdxeVcYrGLnO75ras54OpO757avoit4X8Vab4u0oX2lSMVBw8bjDIfQitqvHvhG2dW8VajpiFNMaQmBcYU9SMUmm/ELxt4p+0WvhrTLZ57WZxNM52qADwoyetONdcqct2XDErkTlu+3kexUV594g8fanolrpmlR2Ed14lvkBa3TOyM+pqjf698RPDNp/amr2Nle2SczxQH5o17kYPNaOtFGjxEU9npvpsej399b6Zp897eyCK3gQvI5H3VHU1Boms2uv6TFqNhuNvMMoWGCRXEeONcuvEHwnn1Pw6IXs7i1kN15p+ZExzj361X+E11rVr4Phm1RbZNFhtS8Uin5+MdefTNL2v7xRW1he3/AHqitrXPTqK8vsvGPjDxpPPN4Qsra20yFyiXNz1lI9MmtDw5471NPFA8M+MrKO01B1zBLEfkm/8Ar01Wi2NYiDa7Pr0PQKK4Xxd45v7HxDB4b8L2SXurTLucyH5IlxnJ/Dmsm+8XeMvBctvdeLbS1udMmcJJLb/eiJ+hodaKb8gliIRb8tz1CiuI8Y/EH+xZLHT9DthqGqaiM28WflA9Tise/wBe+IvhuyOq6rY2V7ZxjdPDCfmjXuRg9qJVop27DlXhFtb23O58T64PDfhu81ZojMLZN5QHGal8P6sNd0Cz1NY/KFzEsgQnO3IziuQ8Za7a+I/gvqOp2JzFNbZweqnIyDW38PP+Se6N/wBeqf8AoIoU26lltYUajlVsnpa50tFFFbHQFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFAHhX7Nn/AB9+M/8Ar9i/nLXuteFfs2f8ffjP/r9i/nLXutABXhP7Lv8AyL+v/wDX2n8mr3avCf2Xf+Rf1/8A6+0/k1AHu1FFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQBykfjLT77xvdeFLq1KyxLuVpcbZRjPApmr/C/wprAYy6YkErf8tYDtaofG3w7g8U3MOo2N2+narbjEdzGSMjqAcVh/wDCJ/E1ovsj+K7MQdDIFbfj67c5rllzXanG5xy5ruNSHMumxU+GL3eh+Pdb8Ki8e8sLUB4mY52E8/8A1q63w/4q0rxvPqOnz2SrJZPskhnAJOc8j8qk8E+BrXwfbzuJnu7+6O64upOWc+n0rG8S/DCS88QNr3hbU20nUn/1mCQjn1OKUY1IQVl8vIUI1adNWV/Ly/4BY134SeFdSt5ZLe0/s6faSs1u23B9TWV8JtXvr3wrq1hfzNcLp8zwxTN3Udv6/jTZvBfxF1WI2ereKrZLRhtkNupV2Xvziu18O+E7Lwx4c/srTujAl5G6uxHLGiMG580Y2/UUIN1OeMeVfmcR8Bf+RVv/APr6P9a9UryLSPhZ4u0CCSDSPFENtFI+8qqt1/KtrTfCHji21S1nvfFaT28cqtLEA3zqDyOncUUZThBRcWOhKdOmoOD09D0OvHviDptrrHxm8P2OoRCa3mhYOh78E17DXH6z4Ln1T4haX4iS6jSOxRlaIg7myMcVrWi5xSXdGuIg5xSS6oyPEfwZ8O32jypo9otleqpMTqeCfQ+1V/hH4hg8u48N39lDYatZEhlRdvmgcE/WvT64LxJ8O59Q8aWfiXQb2OxvIT++DA4l/L2zUSpcklOmvUznR9nNVKS9V5HIeILXV7r49vHpl9HY3LW4+zyypuGPL5A5HvW9qvhnxvNpVxHqfii0FoyESl4CBt/76rd8Z+BP+EnktNQtLs2GsWYHlXCZx64PtmsK98FeO/ENqNN8ReJLT+ziQJRbRFXkHpnArJ02nLRu/mZOlKLkrN37P8zmvE+jNofwPtLKO+S/t47zc80Q+UqXzivZdEMbaBYGHHl/Z49uP90VQbwfpTeD/wDhG/J/0HyvLx3z/e+uea5C18GePdFtP7M0PxLaf2cMiP7RGWkjX0zg1pGMqcrpX0RpGEqMrqN1ZLTyH/EfVdMv/AviOz0aWN7q2Ki7SIYIO8dfxrqPATwP4E0k2m3y/syjj1xz+uap+GPAFloOgXljdyG+m1DJvJ5OTIf8mufs/AfjHwv5lr4P8QWyac7lkhvIy5iz6cGhc8Zc7XToNe0jNVHHdW06FTxKUf4/6CLXmZYgZ9v93J607wuqt8ffEBIBK2oIPpyK6Hwh4AOh6tPrmtXx1LWLgbWmP3UHotT6R4Mm034ian4je5jeK9hEaxAHcvIP9KlU5XUmutyFSm2pNfav+Bzfxk+XUfC0k/8Ax6Let5ueg+71r0yQp9icvjy/LOfTGKyvFnhez8XaFJpt9lQx3JIv3o27EVx8Xgzx4bIaPceKLc6XjYXVD5xT03Y/rWnvQm2le5q+anUlJK9yD4KFCniXyceX/asm3HTHGK9Srjvh54Gk8D2d/bvdLcJc3BlQrnKrgAA578V2NVRi400mXh4yjSSlueG/8IxYeKvjhrVnqbTrEkQceTJsOeO9dkvwW8KhgXN/KB/C9xkH9Kv6X4Jn0/4jah4la6jaK7i2CIA7l6f4V2NZ06MdXNdWZUsPGzc463Zl2+j2Gh+H5bLS7ZLeBImwiD2rhPggijRtbYAbjqb5P4CvS54/OtpIgcF0K59MiuY8BeEJvB9hfW89ylwbq6acFAflB7c1pKD9pFpaK5pKD9rFpaK5yLkR/tIKb3GGsMQ7vXPGP1r0jxC0SeGtSNxjy/ssm7PptNYXjTwJH4omtr+yumsNVszmC5T+Rx2rBvPBXjrxDbjT/EniS1/s7IEgtIyryAe+BWa5ocyte5klOnzRUb3ehh+Fw4/Z618nPltHcGLP93aK1tHWVv2eGFvnzPsfGPwz+ldufCting2Tw3bDybR7cwZHXB6mud8D+Ctf8NLLp+q6rbXujGFo47dVO5SSOpI9M1Kpyi0vKxKoyi4r+7YsfCNoG+GWl/Z9vAcNjsd7da534mFJPiV4PjtP+PsTOXx1x8uP61bh+H3ibwxeXB8D65Bb2U7lza3abghP93g1o+Gvh9cWniI+IvFOojU9WxtQqMRxD/ZFFpygqdu34By1JU40uW1ra9NDG8M/J8ffEAvcea1qPJ3fVcY/CvQ9d1HTNK0w3WuPHHaqwBaUZAPauc8XeApdZ1i313Qr/wDs3WLcYE2PlcdMNj2rJm8BeKfE1zbp431y3uNPgcP9mtEKeYR68CqXPBOKV9So+0ppxUb3enbXuZj3FvN+0JZ3DMrW81gptGxgE47fhXp2vNCnh6/a5wIRbvv3dMbTmue8Y+AbfxIlpc2E50/UrH/j2uI+MD0OO1Yd54L8d+ILUab4h8S2o084En2WIq8i+mcChc8OZWvcFz0+Zct76nL6GJB+zvrxb/VtPKY8+ny16f8ADz/knujf9eqf+gimal4Lgl+Hs3hfSmW3jaHy0dvX1NanhrSX0Lw3Y6ZJIsrW0Kxl16HAxTp05Qkr9h0aUoTV+isalFFFdJ2BRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQB4V+zZ/x9+M/+v2L+cte614V+zZ/x9+M/wDr9i/nLXutABXhP7Lv/Iv6/wD9fafyavdq8J/Zd/5F/X/+vtP5NQB7tRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFAHhX7Nn/H34z/AOv2L+cte614V+zZ/wAffjP/AK/Yv5y17rQAV4T+y7/yL+v/APX2n8mr3avCf2Xf+Rf1/wD6+0/k1AHu1FFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAeFfs2f8AH34z/wCv2L+cte614V+zZ/x9+M/+v2L+cte60AFeE/su/wDIv6//ANfafyavdq8J/Zd/5F/X/wDr7T+TUAe7UUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQB4V+zZ/x9+M/+v2L+cte614V+zZ/x9+M/+v2L+cte60AFeE/su/8AIv6//wBfafyavdq+UfhN4N8QeLvC+qR+HPELaKYb1TIylhv4b0oA+rqK8G/4Un8Q/wDoo83/AH1JUifBr4jRrhfiPJj33mgD3WivDP8AhTvxH/6KO/5PR/wp34j/APRR3/J6APc6K8M/4U78R/8Aoo7/AJPR/wAKd+I//RR3/J6APc6K8M/4U78R/wDoo7/k9H/CnfiP/wBFHf8AJ6APc6K8M/4U78R/+ijv+T0h+DvxJwdvxHbPbIegD3SivB/+FOfE/wD6KQv/AHzJR/wpz4n/APRSF/75koA94orwf/hTnxP/AOikL/3zJT4/hF8UoxhfiRH+MbmgD3WivDf+FTfFT/opEX/fp6P+FTfFT/opEX/fp6APcqK8N/4VN8VP+ikRf9+no/4VN8VP+ikRf9+noA9yorw3/hU3xU/6KRF/36ej/hU3xU/6KRF/36egD3KivDf+FTfFT/opEX/fp6T/AIVP8VP+ijxf9+moA9zorwf/AIVX8Wv+igR/98NR/wAKr+LX/RQI/wDvhqAPeKK8H/4VX8Wv+igR/wDfDU+P4X/FyPO34gRc+sZNAHutFeG/8K1+L3/RQIP+/P8A9aj/AIVr8Xv+igQf9+f/AK1AHuVFeG/8K1+L3/RQIP8Avz/9aj/hWvxe/wCigQf9+f8A61AHuVFeG/8ACtfi9/0UCD/vz/8AWo/4Vr8Xv+igQf8Afn/61AHuVFeG/wDCtfi9/wBFAg/78/8A1qP+Fa/F7/ooEH/fn/61AHuVFeEH4c/GMHjxzCffyx/hSf8ACufjJ/0PMP8A3wP8KAPeKK8H/wCFc/GT/oeYf++B/hTk+HvxljbK+OYM+8QP9KAPdqK8N/4QP40f9Dzbf9+V/wAKP+ED+NH/AEPNt/35X/CgD3KivDf+ED+NH/Q823/flf8ACj/hA/jR/wBDzbf9+V/woA9yorw3/hA/jR/0PNt/35X/AAo/4QP40f8AQ823/flf8KAPcqK8N/4QP40f9Dzbf9+V/wAKP+ED+NH/AEPNt/35X/CgD3KivCW8DfGwMQvjO3I9fKT/AApP+EH+Nv8A0OVv/wB+0/woA93orwj/AIQf42/9Dlb/APftP8KVfBPxuRgw8ZW2R6xIf6UAe7UV4d/wiPxx/wChxtP+/Ef+FH/CI/HH/ocbT/vxH/hQB7jRXh3/AAiPxx/6HG0/78R/4Uf8Ij8cf+hxtP8AvxH/AIUAe40V4d/wiPxx/wChxtP+/Ef+FH/CI/HH/ocbT/vxH/hQB7jRXh3/AAiPxx/6HG0/78R/4Uf8Ij8cf+hxtP8AvxH/AIUAe40V4U/hT46q2F8WWrD18qIf0pv/AAivx3/6Gq1/79Rf4UAe70V4R/wivx3/AOhqtf8Av1F/hSjwv8d1YEeKrXI/6ZRf4UAe7UV4d/wj/wAe/wDoarL/AMB4P/iaP+Ef+Pf/AENVl/4Dwf8AxNAHuNFeHf8ACP8Ax7/6Gqy/8B4P/iaP+Ef+Pf8A0NVl/wCA8H/xNAHuNFeHf8I/8e/+hqsv/AeD/wCJo/4R/wCPf/Q1WX/gPB/8TQB7jRXh3/CP/Hv/AKGqy/8AAeD/AOJo/wCEf+Pf/Q1WX/gPB/8AE0Ae40V4W+hfH9T8niazcevkwD/2Wm/2J+0D/wBDHZ/9+rf/AOJoA92orwn+xP2gf+hjs/8Av1b/APxNH9iftA/9DFZ/9+rf/wCJoA92orw/+yfj5/0G7D/v3D/hR/ZXx8/6Ddh/37h/woA9worw/wDsr4+f9Buw/wC/cP8AhR/ZXx8/6Ddh/wB+4f8ACgD3CivD/wCyvj5/0G7D/v3D/hR/ZXx8/wCg3Yf9+4f8KAPcKK8P/sr4+f8AQbsP+/cP+FH9lfHz/oN2H/fuH/CgD3CivDH0z4/rjZq9i/8AwCAf0pn9nftBf9BOx/KD/CgD3aivCf7O/aC/6Cdj+UH+FH9nftBf9BOx/KD/AAoA92orw8Wfx+A5vNPPv+5o+yfH7/n707/yDQB7hRXh/wBk+P3/AD96d/5Bo+yfH7/n707/AMg0Ae4UV4f9k+P3/P3p3/kGj7J8fv8An707/wAg0Ae4UV4f9k+P3/P3p3/kGj7J8fv+fvTv/INAHuFFeGva/tAKvyXOnufTMIpnkftB/wDPTT/++4KAD9mz/j78Z/8AX7F/OWvda8B/ZeF0D4v+24837TBvxj72Zc179QAV4T+y7/yL+v8A/X2n8mr3avCf2Xf+Rf1//r7T+TUAe7UUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQB4V+zZ/x9+M/wDr9i/nLXuteFfs2f8AH34z/wCv2L+cte60AFeE/su/8i/r/wD19p/Jq92rwn9l3/kX9f8A+vtP5NQB7tRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRVTVYbu40q4i02ZYLpkIikbop9a8w1nS/iRo2i3epTeJbd47WJpWVd2SAPpWc5uHS5jUqOH2Wz1qivGvC8PxF8U6BDqtr4jgijlJwsm7Ix9BXepqdz4O8Dte+Lr1Lq4t1YvJH/AMtDk7VGe/QVMKvMrtWRMK3OuZppdzqKK8n02T4gePYv7St79NB02Q/uETPmMPWotS1bxt8N7iC71q9XW9HdwkrnO+PPfmp9urc1nbuT9ZVuZxdu567RXE/EDxNcWXw2bWtCuPLeTY0cg9DXN6NpfxI1nRbTUofEtukd1Esqq27IBH0qpVbS5UrlSrpS5Um+p61RXkF74n8bfD3U7NvFk1tqWlXMgRpYc5T15I6969cikWaFJU5V1DD6GqhUU7rZounVU21azQ+iiitDUKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooA8K/Zs/4+/Gf/X7F/OWvda8K/Zs/4+/Gf/X7F/OWvdaACvCf2Xf+Rf1//r7T+TV7tXhP7Lv/ACL+v/8AX2n8moA92ooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigArn/AB5/yT/W/wDrzk/lXQVz/jz/AJJ/rf8A15yfyqJ/AyKnwP0Mb4Pf8k1sPq1Yfx4kdtD0ezDFYrq82SY9AARW58Hv+Sa2H1am/F3w5P4g8FO1ipe6sn8+NR1OOuPwFc7TeGsuxySi5YSy7HZadDHb6XbQwqFRIlAA7cU68srbULVre9gjnhbG6ORcg4Oelcp4G8eaX4g0O3SW6jgv4UCTwSNtKsOO/as/4jfEGHSNLOn+H7kT6zcuqQpCdxTkcn+Va+1goc3Q3damqfPfQd8YYYrb4XXMVvGsUaOgVEXAA56CsHwv8Y/C+k+FNNsLuScT21ukbgRMRkD6Ve+Ii6gvwRX+2ZPMviIzMwGOSSf5V1PgWxtH8BaKz2sLMbOMkmMEnisfedb3dNDnfPKv7jtouh5r4s8RTfFiax0Pw3p1x9k84PPdyIQqj+le2WkAtrOGAf8ALNAv5Cljghh/1MSR/wC6oFSVvTpuLcpO7Z0U6Ti3KTu2FFFFam4UUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQB4V+zZ/wAffjP/AK/Yv5y17rXhX7Nn/H34z/6/Yv5y17rQAV4T+y7/AMi/r/8A19p/Jq92rwn9l3/kX9f/AOvtP5NQB7tRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABVfULC31TTp7G8UvBcIY5FBxkHrzViijcHroUNF0Wy8P6XHp+lxmK2j+6pYtj8TV+iikkkrISSSsjjtb+FfhTXrprm707y5mOWaBzHk+4HWp/Dvw38M+GbgXGm2AM46SysXZfpnpXVUVHsoX5ramfsafNzcquZ+t6HY+ItLfT9ViMts5BZQxXke4qxp9hb6Xp0FjZqUgt0Ecak5wB05qxRV2V7mnKr36hRRRTGFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFAHhX7Nn/AB9+M/8Ar9i/nLXuteFfs2f8ffjP/r9i/nLXutABXyp8F/inoPw+0rVbfXEume6uA8fkRhhgZznJHrX1XXz7+zXo+manoOutqWnWl2yXaBTcQLIV4bpkUAdH/wANLeCf+eOp/wDfhf8A4qj/AIaW8E/88dT/AO/C/wDxVek/8Ip4d/6AGl/+Acf+FH/CKeHf+gBpf/gHH/hQB5t/w0t4J/546n/34X/4qj/hpbwT/wA8dT/78L/8VXpP/CKeHf8AoAaX/wCAcf8AhR/winh3/oAaX/4Bx/4UAebf8NLeCf8Anjqf/fhf/iqP+GlvBP8Azx1P/vwv/wAVXpP/AAinh3/oAaX/AOAcf+FH/CKeHf8AoAaX/wCAcf8AhQB5t/w0t4J/546n/wB+F/8AiqP+GlvBP/PHU/8Avwv/AMVXpP8Awinh3/oAaX/4Bx/4Uf8ACKeHf+gBpf8A4Bx/4UAebf8ADS3gn/njqf8A34X/AOKo/wCGlvBP/PHU/wDvwv8A8VXpP/CKeHf+gBpf/gHH/hR/winh3/oAaX/4Bx/4UAebf8NLeCf+eOp/9+F/+Ko/4aW8E/8APHU/+/C//FV6T/winh3/AKAGl/8AgHH/AIUf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/AJ46n/34X/4qj/hpbwT/AM8dT/78L/8AFV6T/wAIp4d/6AGl/wDgHH/hR/winh3/AKAGl/8AgHH/AIUAebf8NLeCf+eOp/8Afhf/AIqj/hpbwT/zx1P/AL8L/wDFV6T/AMIp4d/6AGl/+Acf+FH/AAinh3/oAaX/AOAcf+FAHm3/AA0t4J/546n/AN+F/wDiqP8AhpbwT/zx1P8A78L/APFV6T/winh3/oAaX/4Bx/4Uf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/njqf/fhf/iqP+GlvBP/ADx1P/vwv/xVek/8Ip4d/wCgBpf/AIBx/wCFH/CKeHf+gBpf/gHH/hQB5t/w0t4J/wCeOp/9+F/+Ko/4aW8E/wDPHU/+/C//ABVek/8ACKeHf+gBpf8A4Bx/4Uf8Ip4d/wCgBpf/AIBx/wCFAHm3/DS3gn/njqf/AH4X/wCKo/4aW8E/88dT/wC/C/8AxVek/wDCKeHf+gBpf/gHH/hR/wAIp4d/6AGl/wDgHH/hQB5t/wANLeCf+eOp/wDfhf8A4qj/AIaW8E/88dT/AO/C/wDxVek/8Ip4d/6AGl/+Acf+FH/CKeHf+gBpf/gHH/hQB5t/w0t4J/546n/34X/4qj/hpbwT/wA8dT/78L/8VXpP/CKeHf8AoAaX/wCAcf8AhR/winh3/oAaX/4Bx/4UAebf8NLeCf8Anjqf/fhf/iqP+GlvBP8Azx1P/vwv/wAVXpP/AAinh3/oAaX/AOAcf+FH/CKeHf8AoAaX/wCAcf8AhQB5t/w0t4J/546n/wB+F/8AiqP+GlvBP/PHU/8Avwv/AMVXpP8Awinh3/oAaX/4Bx/4Uf8ACKeHf+gBpf8A4Bx/4UAebf8ADS3gn/njqf8A34X/AOKo/wCGlvBP/PHU/wDvwv8A8VXpP/CKeHf+gBpf/gHH/hR/winh3/oAaX/4Bx/4UAebf8NLeCf+eOp/9+F/+Ko/4aW8E/8APHU/+/C//FV6T/winh3/AKAGl/8AgHH/AIUf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/AJ46n/34X/4qj/hpbwT/AM8dT/78L/8AFV6T/wAIp4d/6AGl/wDgHH/hR/winh3/AKAGl/8AgHH/AIUAebf8NLeCf+eOp/8Afhf/AIqj/hpbwT/zx1P/AL8L/wDFV6T/AMIp4d/6AGl/+Acf+FH/AAinh3/oAaX/AOAcf+FAHm3/AA0t4J/546n/AN+F/wDiqP8AhpbwT/zx1P8A78L/APFV6T/winh3/oAaX/4Bx/4Uf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/njqf/fhf/iqP+GlvBP/ADx1P/vwv/xVek/8Ip4d/wCgBpf/AIBx/wCFH/CKeHf+gBpf/gHH/hQB5t/w0t4J/wCeOp/9+F/+Ko/4aW8E/wDPHU/+/C//ABVek/8ACKeHf+gBpf8A4Bx/4Uf8Ip4d/wCgBpf/AIBx/wCFAHm3/DS3gn/njqf/AH4X/wCKo/4aW8E/88dT/wC/C/8AxVek/wDCKeHf+gBpf/gHH/hR/wAIp4d/6AGl/wDgHH/hQB5t/wANLeCf+eOp/wDfhf8A4qj/AIaW8E/88dT/AO/C/wDxVek/8Ip4d/6AGl/+Acf+FH/CKeHf+gBpf/gHH/hQB5t/w0t4J/546n/34X/4qj/hpbwT/wA8dT/78L/8VXpP/CKeHf8AoAaX/wCAcf8AhR/winh3/oAaX/4Bx/4UAebf8NLeCf8Anjqf/fhf/iqP+GlvBP8Azx1P/vwv/wAVXpP/AAinh3/oAaX/AOAcf+FH/CKeHf8AoAaX/wCAcf8AhQB5t/w0t4J/546n/wB+F/8AiqP+GlvBP/PHU/8Avwv/AMVXpP8Awinh3/oAaX/4Bx/4Uf8ACKeHf+gBpf8A4Bx/4UAebf8ADS3gn/njqf8A34X/AOKo/wCGlvBP/PHU/wDvwv8A8VXpP/CKeHf+gBpf/gHH/hR/winh3/oAaX/4Bx/4UAebf8NLeCf+eOp/9+F/+Ko/4aW8E/8APHU/+/C//FV6T/winh3/AKAGl/8AgHH/AIUf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/AJ46n/34X/4qj/hpbwT/AM8dT/78L/8AFV6T/wAIp4d/6AGl/wDgHH/hR/winh3/AKAGl/8AgHH/AIUAebf8NLeCf+eOp/8Afhf/AIqj/hpbwT/zx1P/AL8L/wDFV6T/AMIp4d/6AGl/+Acf+FH/AAinh3/oAaX/AOAcf+FAHm3/AA0t4J/546n/AN+F/wDiqP8AhpbwT/zx1P8A78L/APFV6T/winh3/oAaX/4Bx/4Uf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/njqf/fhf/iqP+GlvBP/ADx1P/vwv/xVek/8Ip4d/wCgBpf/AIBx/wCFH/CKeHf+gBpf/gHH/hQB5t/w0t4J/wCeOp/9+F/+Ko/4aW8E/wDPHU/+/C//ABVek/8ACKeHf+gBpf8A4Bx/4Uf8Ip4d/wCgBpf/AIBx/wCFAHm3/DS3gn/njqf/AH4X/wCKo/4aW8E/88dT/wC/C/8AxVek/wDCKeHf+gBpf/gHH/hR/wAIp4d/6AGl/wDgHH/hQB5t/wANLeCf+eOp/wDfhf8A4qj/AIaW8E/88dT/AO/C/wDxVek/8Ip4d/6AGl/+Acf+FH/CKeHf+gBpf/gHH/hQB5t/w0t4J/546n/34X/4qj/hpbwT/wA8dT/78L/8VXpP/CKeHf8AoAaX/wCAcf8AhR/winh3/oAaX/4Bx/4UAebf8NLeCf8Anjqf/fhf/iqP+GlvBP8Azx1P/vwv/wAVXpP/AAinh3/oAaX/AOAcf+FH/CKeHf8AoAaX/wCAcf8AhQB5t/w0t4J/546n/wB+F/8AiqP+GlvBP/PHU/8Avwv/AMVXpP8Awinh3/oAaX/4Bx/4Uf8ACKeHf+gBpf8A4Bx/4UAebf8ADS3gn/njqf8A34X/AOKo/wCGlvBP/PHU/wDvwv8A8VXpP/CKeHf+gBpf/gHH/hR/winh3/oAaX/4Bx/4UAebf8NLeCf+eOp/9+F/+Ko/4aW8E/8APHU/+/C//FV6T/winh3/AKAGl/8AgHH/AIUf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/AJ46n/34X/4qj/hpbwT/AM8dT/78L/8AFV6T/wAIp4d/6AGl/wDgHH/hR/winh3/AKAGl/8AgHH/AIUAebf8NLeCf+eOp/8Afhf/AIqj/hpbwT/zx1P/AL8L/wDFV6T/AMIp4d/6AGl/+Acf+FH/AAinh3/oAaX/AOAcf+FAHm3/AA0t4J/546n/AN+F/wDiqP8AhpbwT/zx1P8A78L/APFV6T/winh3/oAaX/4Bx/4Uf8Ip4d/6AGl/+Acf+FAHm3/DS3gn/njqf/fhf/iqP+GlvBP/ADx1P/vwv/xVek/8Ip4d/wCgBpf/AIBx/wCFH/CKeHf+gBpf/gHH/hQB5t/w0t4J/wCeOp/9+F/+Ko/4aW8E/wDPHU/+/C//ABVek/8ACKeHf+gBpf8A4Bx/4Uf8Ip4d/wCgBpf/AIBx/wCFAHm3/DS3gn/njqf/AH4X/wCKo/4aW8E/88dT/wC/C/8AxVek/wDCKeHf+gBpf/gHH/hR/wAIp4d/6AGl/wDgHH/hQB4x+zDeR3snjCWHdte5gkGR2JlxXvteEfs0okdz4zVFVQLyIAAYwMy17vQAV4T+y7/yL+v/APX2n8mr3avCf2Xf+Rf1/wD6+0/k1AHu1FFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUV5j8OtZ1HUPH3ie2vb2eeC3kURRyOSqdeg7Vi6ouveIvjBqOiWPiG806CKJXURSsAOB2rn9v7qaW7scv1hcqklu7HtFFeXyfDrxhBGZLPxvePKoyqzSMVJrQ+GPjDUtc/tDSPEIX+0tNfY7gAbx0PT0qlVfMoyVrlRrPmUZRtc9AooorY6AooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooA8K/Zs/4+/Gf/AF+xfzlr3WvCv2bP+Pvxn/1+xfzlr3WgArwn9l3/AJF/X/8Ar7T+TV7tXhP7Lv8AyL+v/wDX2n8moA92ooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKAPJPhd/yUnxd/11X+tY1/4jXwx8dNUvXs5rsGFV2Q9eg5rZ+F3/ACUnxd/11X+tLo4B/aI1bIz/AKMOv0FecruEbfzf5nlJN04W/mf6lyb4wyyxlNO8L6hNcMMIp45/KrHws8MapYTanr3iGLyL7U5N/kkYKDOTkflXouxR0UflS11qm+ZSk72O2NGXMpTlewUUUVsdAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAeFfs2f8ffjP/r9i/nLXuteFfs2f8ffjP8A6/Yv5y17rQAV4T+y7/yL+v8A/X2n8mr3avCf2Xf+Rf1//r7T+TUAe7UUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFAFCx0PTdNvLi7srSOGe5OZXUcv9aI9E06HV5NUjtY1vZF2vMB8xFX6KXKuxPLHsFFFFMoKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigDwr9mz/j78Z/8AX7F/OWvda8K/Zs/4+/Gf/X7F/OWvdaACvEdN/Z/1nQZLkeHPiNfabb3D72ijsj+GSJRnr6V7dRQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQB5B/wp/xt/wBFa1P/AMA2/wDj1H/Cn/G3/RWtT/8AANv/AI9Xr9FAHkH/AAp/xt/0VrU//ANv/j1H/Cn/ABt/0VrU/wDwDb/49Xr9FAHkH/Cn/G3/AEVrU/8AwDb/AOPUf8Kf8bf9Fa1P/wAA2/8Aj1ev0UAeQf8ACn/G3/RWtT/8A2/+PUf8Kf8AG3/RWtT/APANv/j1ev0UAeQf8Kf8bf8ARWtT/wDANv8A49R/wp/xt/0VrU//AADb/wCPV6/RQB5B/wAKf8bf9Fa1P/wDb/49R/wp/wAbf9Fa1P8A8A2/+PV6/RQBwfwu+GK/Da01FDq8mqz6hIskkrweVjbu7bm/vHvXeUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQB/9k=)

Figure : 4 Layers In The SSL Protocol Stack (Bhakhra, 2023)

### Justification

**Causes Of Vulnerabilities Exists In The Victim Machine**

Based on the screenshot in Figure 14, the vulnerability that existed in the victim machine is due to the outdated version of SSL Protocol enabled in the machine. SSL Version 2 and 3 were initially introduced back in the years 1995 and 1996 respectively, the latest release of SSL is TLS (Transport Layer Security), which is released in the year 2018 (Bhakhra, 2023). Because they are impacted by cryptographic laws, previous versions of SSL are unsafe. Examples include an insecure padding method that uses CBC ciphers, session renegotiation, and insecure resumption strategies. In 2015, the National Institute of Standards and Technology (NIST) announced that SSL Version 3 Protocol is no longer being accepted and used to protect sensitive data and information such as online transactions (PCI SSC bulletin on impending revisions to PCI DSS, PA-DSS, 2015). Due to the weaknesses of this protocol, all the versions of SSL do not meet the Payment Card Industry (PCI) and Security Standards Council (SSC)’s requirements in terms of its cryptography protocol strength.

**How Attackers Can Exploit The Vulnerability**

A picture containing text, screenshot, diagram, line

Description automatically generated To secure an online transaction using SSL, the handshake protocol is used (Zhang, 2003). The handshake protocol lets the client and server authenticate each other by sending messages. There are 4 phases in this protocol, where the first phase is creating sessions and connections between the client and the server. The second phase is the server authentication where the server sends its certificate to the client, exchange its key with the client, and requests the client certificate. The third phase is the client will send its certificate and exchange its key to the server to be authenticated. In the last phase, the client and server will change their cipher spec to each other and thus completing the handshake protocol. With that, the client and server can now transfer data to each other.

Figure : SSL Handshake Protocol (Bhakhra, 2023)

Based on the figure above, because the change cipher spec message is not secured by the current cipher suite, it is claimed that the SSL Handshake Protocol is insecure (Wagner & Schnier, 1996). Before the handshake is complete, a change cipher specification message is sent to the other side to notify them to update their pending session state to the current (Zhang, 2003). The attackers can exploit the change cipher spec message since it was not protected, and they can modify or delete the message. Once deleted, the client and server will never update their current cipher suite. Examples of attacks that can be performed by the attackers on this vulnerability are cipher suite rollback attacks, key-exchange algorithm rollback attacks, version rollback attacks, POODLE attacks, etc (Wagner & Schnier, 1996).

**Example Vulnerabilities Exploitation By the Attackers In Real World Scenario**

**A picture containing text, font, white, typography

Description automatically generated** The attacker can exploit the vulnerability by conducting a cipher suite rollback attack, which is a type of man-in-the-middle attack. The below figures show an original handshake protocol message and a handshake protocol message that is been exploited by the attackers in a cipher suite rollback attack.

Figure : Original Handshake Protocol Message (Wagner & Schnier, 1996)

**A picture containing text, font, white, typography

Description automatically generated**

Figure : Handshake Protocol Message Exploited By Attackers (Wagner & Schnier, 1996)

Based on the figure above, C denotes the client, M denotes the attacker who acts as the man-in-middle, and S denotes the server. When the attacker exploits the change cipher message, they will receive the change cipher spec message that was intended to send to the server from the client. As the server is expected to receive the message in unencrypted form, a, the attackers will need to recover the encryption key, k, to decrypt the encrypted message, {a}k (Wagner & Schnier, 1996). Once the message is decrypted, the attackers will send the message to the server, and the server will send another encrypted message back to the attackers. The attackers will decrypt the message once again and send it to the client. After the handshake is finished, the client will start to transfer data to the server. As no encryption is used during data transmission, the MAC field of the message authentication field, {m}k, can be stripped off easily by the attackers and they can get all the information about the client, {m} (Wagner & Schnier, 1996). Client’s personal information such as account passwords, bank account numbers, and so on will be exposed to the attackers and this can cause the clients a huge loss. Moreover, the attacker can also send malicious code or viruses to both client and server and infect their device, damaging all the programs and reformatting the hard drives in the device.

## Vulnerability 2: MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (Bernard Ong Yuzhe, TP065754)

### Identification

A screenshot of a computer

Description automatically generated

Figure : MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution

One of the serious flaws found after the results of the vulnerability scanning is remote code execution in DNS resolution. A DNS is utilised to convert domain names into IP addresses so that browsers may access other internet resources, a domain name system (Hasna, 2023). On both internal and external networks, majority of hosts have both a distinct IP address and hostname.

DNS resolution is the process of turning machine-readable IP addresses into human-readable domain names, such as www.example.com. In order for computers and other devices to connect with one another over the internet using domain names—which are simpler to learn and use than IP addresses—domain name system (DNS) resolution is necessary. The architecture of DNS includes the local or subdomain(s), the parent domain, and the domain extension all make up the hostname. These elements work together to provide hosts an approachable persona that clients may connect with (Datadog, 2022).

Remote code execution (RCE) is a sort of security flaw that enables an attacker to remotely execute any code or instructions on a target system without having physical access to the system or any valid log-in credentials (Bugcrowd*,* 2022). In addition, Remote code execution (RCE) in DNS resolution refers to a defect that enables an attacker to run arbitrary code on a target system by taking advantage of a weakness in the DNS resolution procedure.

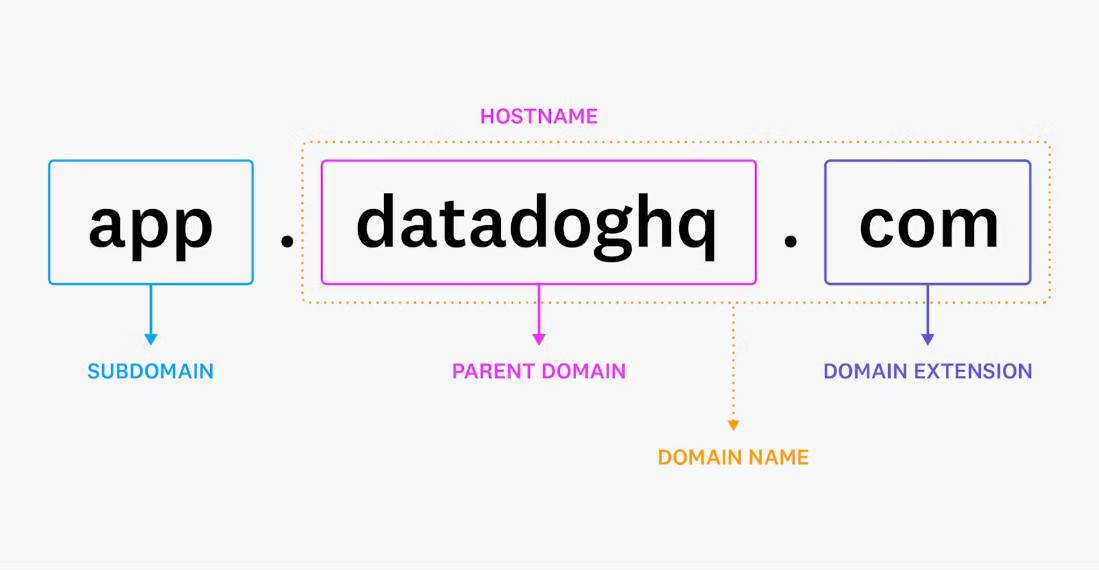


Figure 19: DNS Architecture (Datadog, 2022)

### Justification

**Causes Of Vulnerabilities Exists In The Victim Machine**

Multiple factors can lead to DNS resolution vulnerabilities that allow remote code execution (RCE). Software faults or defects in DNS software and resolvers are one of the main reasons. These mistakes may result from improper coding procedures or insufficient testing, which leaves the system open to intrusion by attackers who can use these flaws to run arbitrary code from a distance (BetaFred, 2023).

DNS server configuration issues are another factor in RCE in DNS resolving (Rudis, 2020). RCE attacks may succeed on DNS servers that are not properly setup or protected. An attacker might utilise a DNS server that is set up to permit zone transfers to unauthorised hosts, for instance, to retrieve the DNS records and insert malicious code. In a similar vein, DNS servers can open themselves up to new RCE vulnerabilities that attackers can use to get into the system if they are not properly patched and updated.

RCE flaws in DNS resolution can also be exploited via malicious DNS entries. Attackers can inject malicious DNS records that can be used to execute arbitrary code on the target machine by taking advantage of flaws in the DNS record format or by using DNS cache poisoning. As a result, the attacker may be able to take complete control of the machine and carry out a number of nefarious tasks.

RCE in DNS resolution can also result via software dependency exploitation. There may be dependencies between DNS servers and resolvers and other software parts, such as libraries and frameworks, which may each contain RCE flaws of their own. Attackers can use these dependencies to remotely execute programmes.

**How Attackers Can Exploit The Vulnerability**

By taking use of flaws or vulnerabilities in the DNS server software or architecture, attackers can utilise DNS resolution vulnerabilities that provide remote code execution. Sending specially crafted DNS requests or replies to the target DNS server that contain malicious data or code is one frequent method used by attackers to take advantage of these vulnerabilities. Following improper validation or sanitization by the DNS server, a buffer overflow or other vulnerability may result, giving the attacker the ability to run arbitrary code.

An attacker can take complete control of the system and potentially access sensitive data once they have executed arbitrary code on the target DNS server. They could even conduct other attacks on networked systems or steal data from other devices using the hijacked DNS server.

Maintaining software updates is the primary method of avoiding remote code execution in DNS resolution; access restrictions and firewalls must be put in place to limit access to the DNS server. By doing this, user may be able to stop hackers from using the DNS server to access the server or network. In order to detect and stop DNS-based attacks before they can take advantage of weaknesses in the DNS server, intrusion detection and prevention methods can also be put in place.

**Example Vulnerabilities Exploitation By the Attackers In Real World Scenario**

The CVE-2008-1447 vulnerability is an illustration of a DNS resolution flaw that might lead to remote code execution. Microsoft's DNS server in Windows Server 2000, 2003, and 2008 was vulnerable to this issue (suse, 2023).

Upon receiving a specifically constructed DNS response from an attacker, the DNS server experienced a buffer overflow, which led to the vulnerability. The length of the DNS name in the response caused the buffer to overflow and could overwrite nearby memory regions with attacker-controlled data.

By providing a specially designed DNS answer to the server, an attacker might take advantage of this vulnerability and run any code with the same rights as the DNS server process. As a result, the attacker could be able to access sensitive data and take full control of the compromised machine.

## Vulnerability 3: MS09-22: Vulnerabilities in Window Print Spooler Could Allow Remote Code Execution (961501) (She Jun Yuan TP065157)

### Identification

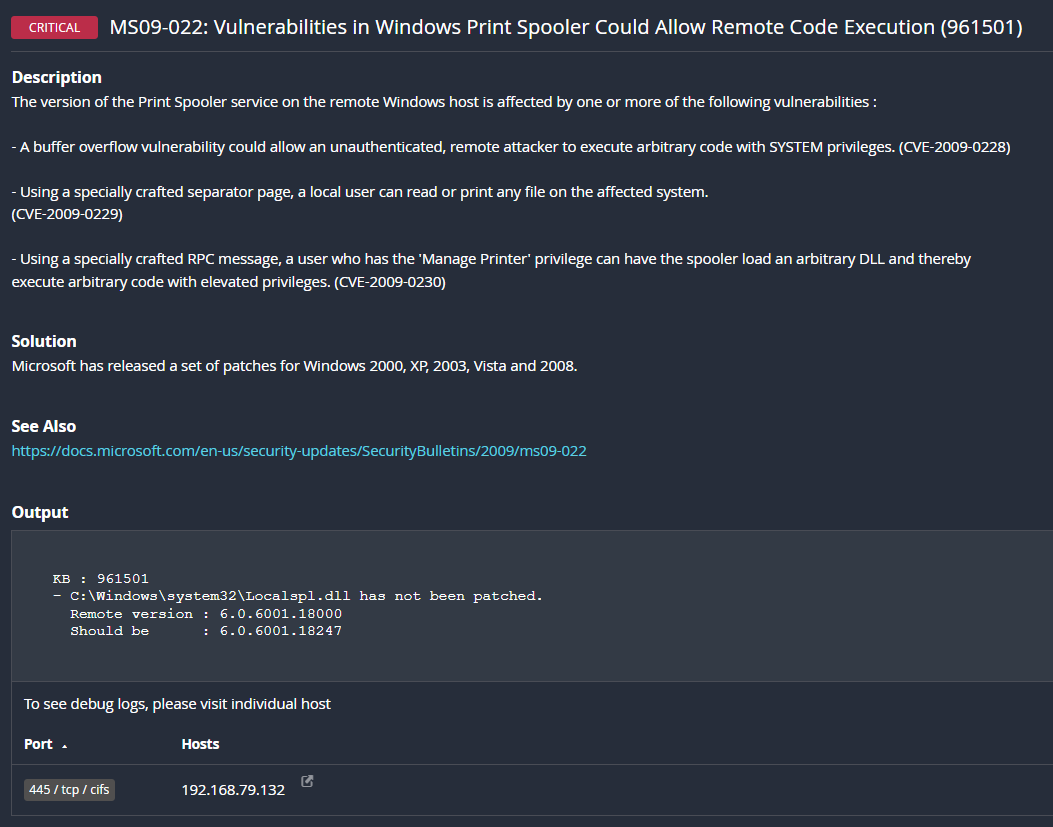
****

Figure : MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)

Another critical vulnerability that has been found in the Windows 2008 victim machine through the vulnerability scanning tool, Nessus is remote code execution that causes by the vulnerabilities in the Windows Print Spooler. This vulnerability, MS09-022 has addressed a set of weaknesses that discovered in the Windows Print Spooler service that might allow the attackers to remotely execute arbitrary code on the Windows 2008 victim machine. When the attackers successfully exploit this weakness of the Windows 2008 victim machine, they may seize total control of this victim machine (BetaFred, 2009).

Windows Print Spooler is a software program that designed to temporarily stores print jobs in memory until the printer is prepared to process and print them (FAQ Article Page | Epson United Kingdom, n.d.). Once the printer is prepared to print, the print jobs will be sent to the printer by the print spooler. Thus, the main function of the Windows Print Spooler is managing the printing process of the computer system, such as identifying the appropriate printer driver, loading it, handling spooling of high-level function calls into a print job, scheduling the print job for execution, and performing other tasks (hickeys, 2021). With this print spooler software, the user can control the print jobs that are now waiting to be printed or remove a print job that is already being handled. This software program will be started up with the system and runs until the operating system is shut down. However, there are some weaknesses of the Windows Print Spooler which will cause this vulnerability, MS09-022, that will allow the attackers to unauthorized access the victim machine.

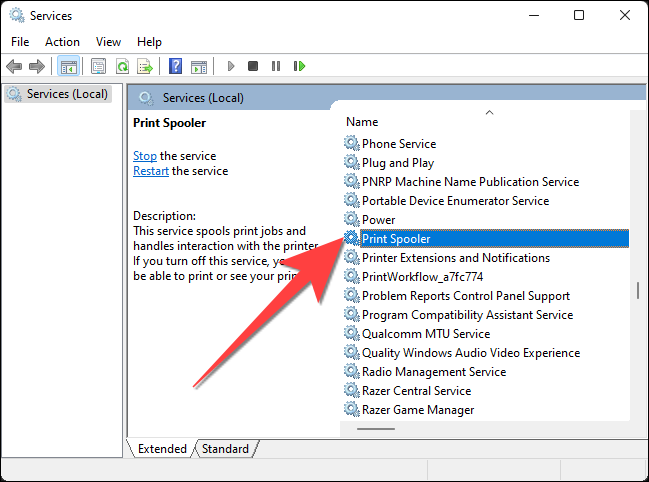


Figure : Windows Print Spooler (Makwana, 2021)

### Justification

**Causes Of Vulnerabilities Exists In The Victim Machine**

This vulnerability is found in the Windows 2008 victim machine and has the severity level of critical because there are some weaknesses that present in the Windows Print Spooler which will cause the remote code execution in the Windows 2008 victim machine. There are total of three weaknesses of the Windows Print Spooler, which are buffer overflow in print spooler weakness, print spooler read file vulnerability, and print spooler load library vulnerability. However, buffer overflow in print spooler vulnerability will not be discussed as this vulnerability does not applicable to Windows 2008 victim machine.

The first vulnerability that is present in the Windows Print Spooler is print spooler read file vulnerability. This flaw in the Windows Print Spooler on the Windows 2008 victim computer enables local users to read whatever files they want via a specially created separator page (Microsoft Corporation, 2009). Even in the absence of administrator access, the users can still conduct this activity. However, the flaw could not be exploited remotely or by unidentified individuals. The root cause of this weakness is the inadequate verification of files that be included with the separator pages in the Windows Printing Spooler. Due to this neglect, the system of Windows 2008 victim machine fails to conduct proper checks of these files, which will lead to the attacker being able to perform remote code execution.

Besides, another factor that causes the MS09-022 vulnerability is the print spooler load library vulnerability. The Windows Print Spooler in the Windows 2008 victim machine will enable the remote authenticated users to obtain access by sending a forged Remote Procedure Call (RPC) message that causes the loading of a DLL file from any location (CVE - CVE-2009-0230, n.d.). Dynamic Link Library (DLL) is a group of compact programs that bigger programs can call upon as needed to carry out certain tasks. The smaller programs, often known as a DLL file, consist of instructions that assist the bigger programs in handling tasks that may not have been its primary purpose when it was created (Lutkevich, 2021). The attackers gain the ability to execute any code with administrative rights after the attackers successfully exploit the vulnerability. With this degree of access, they have total authority and may install unauthorized programs, establish new accounts with elevated privileges, and manipulate, read, change, or delete data as they see fit.

**How Attackers Can Exploit The Vulnerability**

For the attacker to conduct remote code execution on the Windows 2008 victim machine, the attacker will exploit the weaknesses of the Windows Print Spooler, such as print spooler read file and the print spooler load library to access unauthorizedly to the victim machine. However, in order to exploit these vulnerabilities in the Windows Print Spooler, the attacker will require to get the “Manage Printer” privilege. Once the attacker obtains it, he will be able to use the vulnerabilities to conduct remote code execution.

First, to exploit the print spooler read file vulnerability, the system must be logged in for the attacker to use this vulnerability. Once the attacker successfully logs in to the system, the attacker might then create a custom separator page tailored for the print request (BetaFred, 2009). This separator page will be included any system file that the attacker wanted to access or manipulate in the print request. Thus, the attacker might take advantage of this vulnerability and access the Windows 2008 victim machine file without authorization by injecting the malicious separator page into the print request.

Besides, by placing a malicious dynamic link library (DLL) in a location that the print spooler can reach, the attacker can successfully exploit the print spooler load library vulnerability. Then, the attacker will continue his act by building a specially designed Remote Procedure Call (RPC) message and transferring it to the Windows 2008 victim machine. The message would prompt the print spooler to load the DDF and subsequently execute the code with the elevated privileges. The attacker can access the system without authorization and possibly engage in several destructive actions thanks to this elevated execution.

**Example Vulnerabilities Exploitation By the Attackers In Real World Scenario**

In real world scenarios, the attackers will conduct reconnaissance, which is a process of secretly learning about and gathering data about a system (Reconnaissance, 2020). During conducting reconnaissance, the attacker is able to determine a target individual or organization that employs a lot of networked printers and have Windows-based computers with the Windows Print Spooler turned on.

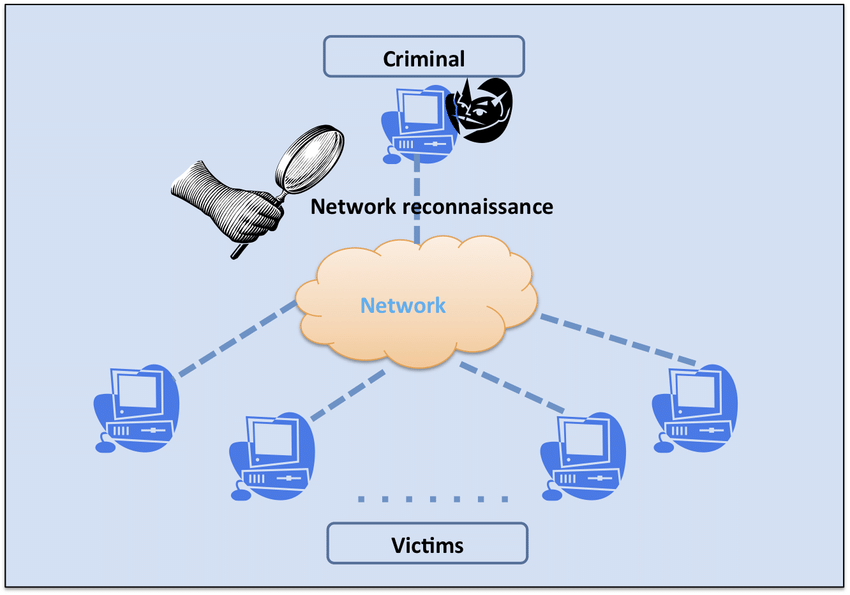


Figure : Reconnaissance

Once the attacker targeted an individual or organization, the attacker will then exploit the weaknesses of the Windows Print Spooler to achieve remote code execution. The attacker can choose various weaknesses that are present in the Windows Print Spooler. For example, the attacker can design a unique separator page specifically for the print request, which this separator will contain the system file that the attacker intends to access or allocating a harmful dynamic link library (DLL) in the location that print spooler can access (BetaFred, 2009).

By exploiting one of the vulnerabilities of the Windows Print Spooler, the attacker will be able to perform remote code execution toward the targeted computer system. After they successfully perform the remote code execution, the attacker can then possibly gain complete control of the targeted computers by using the Print Spooler service's privileges. When the attacker gains unauthorized access to the targeted system, the attackers will start to conduct some cybercrimes such as deleting the programs of the system, changing, and taking important data from the individual or the organization, and so on.

## Vulnerability 4: MS10-009: Vulnerabilities in Windows TCP/IP could allow Remote Code Execution (974145) (Teoh Mae Kay TP065097)

### Identification

A screenshot of a computer program

Description automatically generated with medium confidence

Figure : MS10-009: Vulnerabilities in Windows TCP/IP could allow Remote Code Execution (974145)

Another critical vulnerability that has been found in Windows Server 2008 is vulnerabilities in Windows TCP/IP could allow remote code execution. The bulletin addresses 4 vulnerabilities which are not known at that time publicly or being exploited. MS10-009 will affects TCP/IPV6 specifically. In Windows Server 2008, TCP/IPv6 is enabled by default. For instance, if an attacker specially crafted ICMPv6 packet to an unpatched system and sends to it, the attacker would have the ability to remote code execution on the victim’s system (Miler, 2010).

TCP/IP, short for Transmission Control Protocol/Internet Protocol, is a suite of communication protocols utilised to connect network devices to the internet. It is also employed as a communications protocol in intranets and extranets. TCP/IP ensures reliable end-to-end communication by specifying the way of data should be divided into packets, addressed, transferred, routed, and received at the destination. This suite of protocols plays a fundamental role in enabling data exchange over the internet while facilitating automatic recovery from network component failures and minimizing the need for central supervision.

Within the IP suite, two primary protocols serve as distinct purposes. The first is TCP, which governs the establishment of communication channels between programs across a network. TCP also handles the fragmentation of messages into smaller packets for transmission over the internet, ensuring they are reassembled in the correct order at the destination address (Shacklett et al., 2021).

### Justification

**Causes Of Vulnerabilities Exists In The Victim Machine**

One of the causes of MS10-009 vulnerabilities is ICMPv6 Router Advertisement vulnerability causing remote code execution might happen. The hosts that have IPv6 enabled may exhibit inadequate bounds checking during the processing of specifically crafted ICMPv6 Router Advertisement (RA) packets. This vulnerability could potentially be exploited by a remote attacker to execute arbitrary code on the affected system. These packets are often sent out through routing devices as ICMPv6 packets to notify the network devices on the network prefix to utilised, and the way to direct to external IPv6 requests. When a host receive a RA, the packet updates the records of network prefix. If the network prefix is different, it will add new addresses. Typically, a router solicitation is broadcast by the host asking routers to give RA in order to obtain an IPv6 route. The attack overwhelms the local network with fake advertisements for random routers, hosts and routers update the network configuration, used up all CPU resources, rendering the systems unavailable and unusable (Nassereldeen, 2013).

In addition to the vulnerabilities, there have been instances of remote code execution vulnerabilities in the Windows TCP/IP stack due to Header Memory Descriptor List (MDL) fragmentation. This vulnerability arises when the Windows TCP/IP stack fails to handle specially crafted encapsulating Security payloads (ESP) over UDP datagram fragments when a custom network driver is in use. The MDL is a system-defined structure that employs a list of physical addresses to define a buffer. Direct I/O drivers utilize MDLs to read and write data after receiving a pointer from the I/O manager. While ESP provides confidentiality, authentication, integrity, and anti-replay security for the IP payload, it does not sign the entire packet in transport mode. Only the IP payload is secured, while the IP header remains unprotected. Both the Authentication Header (AH) and ESP can be used independently or together. If an attacker successfully exploits this vulnerability, they could gain control over the affected system. This level of control could enable them to view, modify, or delete data, create new accounts with full user rights, or even install unauthorized programs on the compromised system (BetaFred et al., 2010).

Moreover, Microsoft Windows is susceptible to a denial of service in its TCP/IP processing when selective acknowledgement vulnerability occurred. This vulnerability stems from an error in handling specially crafted TCP packets containing a malformed selective acknowledgment (SACK) value. By sending a small number of these packets to the targeted system, an attacker can cause the affected system to become unresponsive and initiate an automatic restart. Selective acknowledgment (SACK) is utilized for connections with large TCP window sizes. When SACK is enabled, the receiver can inform the sender about the exact data received and identify any gaps in the received data caused by dropped packets. This allows the sender to selectively retransmit the missing data without retransmitting already received data blocks. Prior to the introduction of SACK in the Windows TCP/IP stack with Windows 2000, the receiver could only acknowledge the latest sequence number of contiguous data received or the left edge of the receive window (BetaFred et al., 2010).

**How Attackers Can Exploit The Vulnerability**

For attackers to exploit ICMPv6 Router Advertisement (RA) vulnerability, they need to craft a ICMPv6 packets, and these packets will be delivered to a IPv6 enabled system. The packet is directed to the multicast address FF02::1, which is designated for all-nodes. This indicates that each node will receive and handles the packets. RA packets convey essential information to the nodes, including the prefix, prefix length, and additional parameters such as Maximum Transmission Unit (MTU), relevant to the segment (Network Academy.io, 2020).

A picture containing text, screenshot, font, diagram

Description automatically generated

Figure : IPv6 Router Advertisement Message (Network Academy.io, 2020)

To exploit this vulnerability, the attacker must be located within the same network segment, commonly referred to as being "on-link." However, the presence of tunnelling protocols like ISATAP can enable attackers to deliver a maliciously crafted packet to the target machine, even if they are not physically connected to the same physical link. This means that attackers can leverage tunnelling protocols to remotely exploit the vulnerability, bypassing the requirement of direct physical presence on the same network link (BetaFred et al., 2010).

Furthermore, attackers could take the advantage of header MDL fragmentation vulnerability to achieve remote code execution on the targeted system. Attackers will craft malicious packets that triggered the vulnerability and send them through the network. Packets sending can be done by connecting directly to the targeted system or using network techniques like tunnelling protocols or IP spoofing. Once the targeted system has received the specially crafted packets, the vulnerable Windows TCP/IP stack processes them. The improper handling of packets will lead to buffer overflow, memory corruption or even other vulnerabilities in stack.

Other than that, TCP/IP selective acknowledgment (SACK) could be exploit by attackers by handling acknowledgements of received data from TCP protocol. Attackers will craft malicious packets with manipulated SACK options to exploit the vulnerabilities in the TCP implementation. After delivering the packets through network as they are from a trusted source. Once the targeted system received the packets, the TCP/IP stack will handle them. As improper handling of SACK options will cause network performance degradation, resource exhaustion, or remote code execution. Meanwhile, attackers can use these vulnerabilities to launch further attacks, such as disrupt the functionality of the targeted system.

**Example Vulnerabilities Exploitation By the Attackers In Real World Scenario**

## Vulnerability 5: MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318) (Tay Hui Yee TP064988)

### Identification

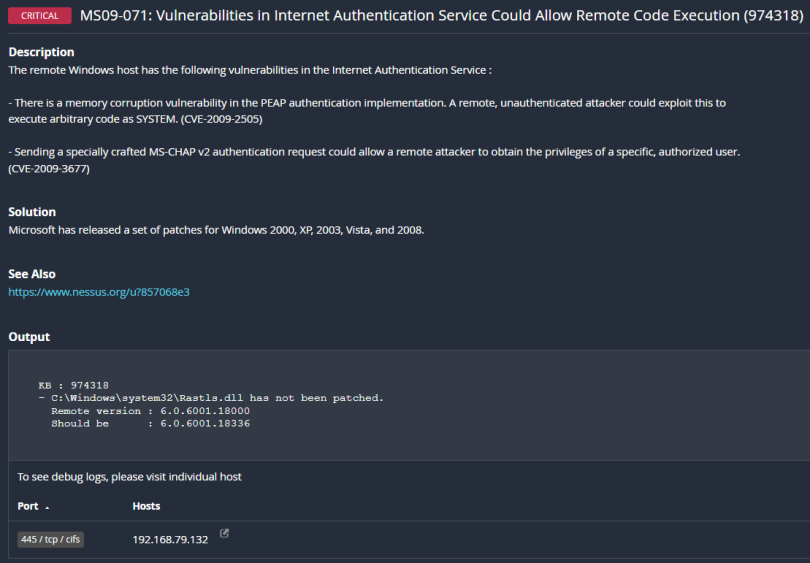


Figure : MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)

A critical issue identified during the vulnerability scanning is the ability for remote code execution to occur in Internet Authentication Service. This security update addresses two vulnerabilities that were privately reported in Microsoft Windows, one of which is particularly severe as it may permit remote code execution. The vulnerability occurs when messages received by the Internet Authentication Service server are improperly copied into memory while processing PEAP authentication attempts.

<https://networkencyclopedia.com/internet-authentication-service-ias/>

Internet Authentication Service, IAS is a service included with Internet Connection Services' Microsoft Remote Access Service (RAS) that provides integrated authorization, authentication, and accounting functionalities for networks. It was a part of Windows 2000 and the Microsoft Windows NT 4.0 Option Pack. The Internet Authentication Service (IAS)'s main purpose is to provide authentication and authorisation services for users connecting remotely to their corporate network. System administrators can also use IAS to monitor connection consumption for corporate accounting and invoicing purposes.

However, servers using either of these services with PEAP and MS-CHAP v2 authentication are at risk of being compromised by attackers who can exploit these vulnerabilities. Successful exploitation of either vulnerability can lead to complete control of the affected system by the attacker.

Protected Extensible Authentication Protocol (PEAP) implementation on the Internet Authentication Service contains a severe vulnerability that could result in remote code execution. The server's inappropriate copying of messages received while performing PEAP authentication attempts is the cause of the vulnerability. machine administrators and users should both take this vulnerability seriously because it might be exploited to give an attacker total control over the vulnerable machine.

Protected Extensible Authentication Protocol (PEAP) is a type of Extensible Authentication Protocol (EAP) protocol that uses Transport Layer Security (TLS) to establish an encrypted communication channel between an authenticating PEAP client, such as a mobile device connected to a wireless network, and a PEAP authenticator, such as an Internet Authentication Service (IAS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify a particular authentication method, but enhances the security of other EAP authentication protocols, like EAP-MS-CHAP v2, by providing a secure TLS channel for their operation. PEAP is commonly used as an authentication method for wireless client computers, but is not supported for virtual private network (VPN) or other types of remote access clients.

### Justification

**Causes Of Vulnerabilities Exists In The Victim Machine**

Insufficient PEAP authentication request validation leads to vulnerabilities in the Internet Authentication Service that permit remote code execution. The vulnerabilities specifically occur when the IAS server mishandles these requests and causes an error during the copying of specific memory structures. Attackers can use this mistake to execute malicious code and take over the vulnerable system.

The use of MS-CHAP v2 authentication, which is vulnerable to various kinds of attacks, makes worse the flaws. These elements work dangerously together to cause serious harm to organisations that depend on the impacted systems for authentication and access control. Organisations should be aware of these vulnerabilities and take the appropriate security upgrades and precautions to reduce the risk of exploitation. Regular security audits and assessments can also aid in locating possible flaws before attackers can use them.

The vulnerability you mentioned, which could allow remote code execution in the Internet Authentication Service (IAS) on a victim machine, could have various causes. Without specific details about the version of IAS or any known vulnerabilities, it's difficult to provide a precise answer. However, I can explain some general factors that can contribute to vulnerabilities in authentication services.

Software Bugs: Vulnerabilities often arise from programming errors or software bugs. These flaws can allow attackers to exploit certain functionalities or bypass security mechanisms in the authentication service. Errors in the code implementation or design flaws can lead to vulnerabilities. These bugs can be exploited by an attacker to execute malicious code on the victim machine.

Lack of Input Validation: If the authentication service does not properly validate user input, it becomes susceptible to attacks such as buffer overflows, SQL injection, or command injection. Attackers can exploit these weaknesses to execute arbitrary code on the target system.

Weak Authentication Mechanisms: Weak authentication methods, such as weak passwords, lack of multi-factor authentication, or inadequate encryption of sensitive data, can make the system more vulnerable. Attackers can easily compromise user credentials or intercept authentication tokens to gain unauthorized access.

Misconfiguration: Incorrectly configuring the authentication service or associated components can introduce vulnerabilities. This can include using default or weak settings, not applying necessary security patches or updates, or failing to implement secure protocols.

Third-Party Libraries or Dependencies: Many authentication services rely on third-party libraries or components. If these dependencies have their vulnerabilities or are not kept up to date, they can serve as entry points for attackers.

Social Engineering: In some cases, vulnerabilities may not be related directly to the authentication service itself but rather to human factors. Attackers can exploit social engineering techniques to trick users or administrators into revealing sensitive information or executing malicious actions.

**How Attackers Can Exploit The Vulnerability**

The PEAP authentication implementation contains a memory corruption bug that is responsible for the CVE-2009-2505 issue. This flaw can be remotely exploited by an attacker without the need for authentication. The attacker can execute any code with SYSTEM-level privileges by taking advantage of the weakness. The attacker has complete control over the targeted system with this degree of access, allowing them to engage in a variety of destructive actions.

An attacker can take advantage of CVE-2009-3677 by providing a well designed MS-CHAP v2 authentication request. The remote attacker can take over the rights of a particular, authorised user after a successful exploit. This effectively gives the attacker the identity and rights of the targeted user, allowing them to get access to confidential data, carry out unauthorised deeds, or jeopardise system security as a whole.

It is critical to remember that these flaws were first discovered in 2009, and that the best way to reduce the dangers associated with them is to keep software and systems updated with security updates.

Attackers can gain remote code execution by exploiting holes in how the server handles PEAP authentication attempts in the Internet Authentication Service. Attackers might be able to take over the system if messages received by the server are erroneously copied into memory. These flaws are particularly dangerous since they give attackers total control over the system they are seeking.

**Example Vulnerabilities Exploitation By the Attackers In Real World Scenario**

<https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack#:~:text=More%20than%2018%2C000%20customers%20of,were%20affected%20by%20this%20attack>.

<https://ollisakersarney.com/blog/cyber-case-study-solarwinds-supply-chain-cyberattack/>

It was revealed in the last month of 2020 that foreign hackers had engaged in a supply chain cyberattack during the previous year with the intention of breaching various public and commercial organisations. The attackers first breached the Texas-based technology company SolarWinds' digital infrastructure, which they then employed to obtain sensitive data from several government agencies and organizations by means of malware-infected software upgrades. Numerous SolarWinds customers were ultimately impacted by the incident, which resulted in overall losses of millions of dollars.

The Tulsa, Oklahoma-based startup SolarWinds offers SaaS solutions for network administration, supply management, and IT infrastructure. They have full access to client data, logs, and workflow specifics as an organisation that deals with IT infrastructure management.

In the last month of 2020, it was disclosed that foreign hackers had carried out a supply chain cyberattack over the past year, with the aim of compromising several federal agencies and private organizations. The attackers initially infiltrated the digital infrastructure of SolarWinds, a Texas-based technology firm, and subsequently used it to gain access to sensitive data from various government departments and organizations via software updates infected with malware. The attack ultimately affected numerous SolarWinds customers and caused millions of dollars in total losses.

The incident has been referred to as one of the most significant and sophisticated cyberattacks in the history of the United States, prompting many organizations to scrutinize security risks arising from their supply chains and software providers. In hindsight, there are several cybersecurity lessons that organizations can glean by examining the details of the SolarWinds attack.

# CONCLUSION

In conclusion, network scanning is selected as scanning method which uses Nessus as a tool. Nessus is selected for scanning the vulnerabilities in the Windows Server 2008 victim machine. There are various vulnerabilities being detected after scanning Windows Server 2008 victim’s machine by using network scanning. The 5 chosen vulnerabilities are SSL Version 2 and 3 Protocol Detection, Remote Code Execution in DNS resolution, Window Print Spooler Could Allow Remote Code Execution, Windows TCP/IP could allow Remote Code Execution and Internet Authentication Service Could Allow Remote Code Execution. Other than SSL Version 2 and 3 Protocol Detection, the other 4 vulnerabilities are remote code execution in different areas. This is because remote code execution is the worst-case scenario as they allow an attacker to take complete control of a system and carry out various malicious actions, such as stealing data, installing malware, or hijacking the system for further attacks. Due to their potential impact, RCE vulnerabilities are considered critical and should be addressed immediately upon discovery.

# REFERENCES

BetaFred, Justinha, wingtofree, mdressman, & v-prhal. (2010, February 9). *Microsoft Security Bulletin MS10-009 - Critical*. Microsoft. <https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-009#executive-summary>

BetaFred. (2009, June 17). *Microsoft Security Bulletin MS09-022 - Critical. Microsoft.* <https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2009/ms09-022>

BetaFred. (2023). *Microsoft Security bulletin MS11-030* . Microsoft . <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030>

Bhakhra, S. (2023, February 26). *Secure Socket Layer (SSL)*. GeeksforGeeks. <https://www.geeksforgeeks.org/secure-socket-layer-ssl/>

Bugcrowd. (2022, July 13). *Remote code execution (RCE)*. <https://www.bugcrowd.com/glossary/remote-code-execution-rce/>

*CVE - CVE-2009-0230*. (n.d.). CVE. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0230>

Datadog. (2022, June 30). *Datadog*. What is DNS Resolution? How DNS Works & Challenges. <https://www.datadoghq.com/knowledge-center/dns-resolution/>

*FAQ Article Page | Epson United Kingdom*. (n.d.). EPSON. <https://www.epson.co.uk/faq/KA-01651/contents?loc=en-us#:~:text=The%20Print%20Spooler%20is%20software>

Hasna. (2023, April 5). *What is DNS and how does it work – A comprehensive guide*. Hostinger Tutorials. <https://www.hostinger.my/tutorials/what-is-dns>

hickeys. (2021, August 1). *Print Spooler - Win32 apps*. Microsoft. <https://learn.microsoft.com/en-us/windows/win32/printdocs/print-spooler>

Itperfection. (2021, January 18). *What is NESSUS and How Does it Work?* ITperfection - Network Security. <https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/>

Kime, C. (2023, March 8). *The 8 Best Vulnerability Scanner Tools for 2023*. eSecurity Planet. <https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/>

Lutkevich, B. (2021, November 18). *What is dynamic link library (DLL)?* SearchWindowsServer. <https://www.techtarget.com/searchwindowsserver/definition/dynamic-link-library-DLL>

Makwana, S. (2021, August 3). *How to Disable the Print Spooler Service on Windows 10.* How-to Geek. <https://www.howtogeek.com/744645/how-to-disable-the-print-spooler-service-in-windows-10/>

Microsoft Corporation. (2009, June 10). NVD - CVE-2009-0229. NIST. <https://nvd.nist.gov/vuln/detail/CVE-2009-0229>

Nassereldeen, A. (2013, December). *ICMPv6 Router Advertisement Flooding*. Research Gate. <https://doi.org/10.13140/2.1.4676.7368>

Network Academy.io. (2020, October 30). *IPv6 Neighbor Discovery Protocol*. NetworkAcademy.io. <https://www.networkacademy.io/ccna/ipv6/neighbor-discovery-protocol#:~:text=Router%20Advertisement%20%2D%20IPv6%20routers%20advertise>

*Nmap vs Nessus | Learn the Top Key Differences and Comparisons*. (2021, September 20). EDUCBA. <https://www.educba.com/nmap-vs-nessus/>

Odogwu, C. (2021, December 4). *What Is Network Scanning and How Does It Work?* Make Use Of. <https://www.makeuseof.com/what-is-network-scanning/#:~:text=Network%20scanning%20is%20the%20process>

*PCI SSC bulletin on impending revisions to PCI DSS, PA-DSS*. (2015, February 13). PCI Security Standards. <https://listings.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revisions_SSL_update.pdf>

Reconnaissance. (2020, October 9). Blumira. <https://www.blumira.com/glossary/reconnaissance/>

RSI Security. (2023, March 9). *7 Types of Vulnerability Scanners*. RSI Security. <https://blog.rsisecurity.com/7-types-of-vulnerability-scanners/>

Rudis, boB. (2020, October 26). *Windows DNS server RCE vulnerability (CVE-2020-1350): Rapid7 blog*. Rapid7. <https://www.rapid7.com/blog/post/2020/07/14/windows-dns-server-remote-code-execution-vulnerability-cve-2020-1350-what-you-need-to-know/>

*Secure Sockets Layer (SSL) protocol*. (2023, April 4). IBM. <https://www.ibm.com/docs/en/ibm-http-server/9.0.5?topic=communications-secure-sockets-layer-ssl-protocol>

Shacklett, M. E., Novotny, A., & Gerwig, K. (2021, July). *TCP/IP: What is TCP/IP and How Does it Work?* TechTarget. <https://www.techtarget.com/searchnetworking/definition/TCP-IP#:~:text=TCP%2FIP%20stands%20for%20Transmission>

SUSE. (2023). *CVE-2008-1447*. <https://www.suse.com/security/cve/CVE-2008-1447.html>

Wagner, D., & Schneier, B. (1996). Analysis of the SSL 3.0 protocol. *The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press*, 29–40. <https://www.schneier.com/academic/archives/1996/11/analysis_of_the_ssl.html>

Wendlandt, D. (2019). *Nessus*. Cmu.edu. <https://www.cs.cmu.edu/~dwendlan/personal/nessus.html>

Zhang, H. L. (2003). Three attacks in SSL protocol and their solutions. In *https://cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/* (COMPSCI 725). Department of Computer Science, The University of Auckland. <https://cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/725zhang.pdf>