**Logo, company name

Description automatically generated**

**INDIVIDUAL ASSIGNMENT**

**TECHNOLOGY PARK MALAYSIA**

**AICT006-4-2-DSF**

**DIGITAL SECURITY AND FORENSICS**

**UCDF 2107ICT(SE)**

**LECTURER: NIK NURUL AIN NIK SUKI**

**HANDOUT DATE: 13rd APRIL 2023**

**HANDIN DATE: 22nd MAY 2023**

**WEIGHTAGE: 20%**

**STUDENT: TAY HUI YEE TP064988**

**INSTRUCTIONS TO CANDIDATES:**

1. **Submit your assignment at the administrative counter.**
2. **Students are advised to underpin their answers with the use references (cited using the Harvard Name System of Referencing).**
3. **Late submission 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 soft copy of the written assignment and source code (where appropriate) should be on a CD in an envelope / CD cover and attached to the hardcopy.**

Table of Contents

[1.0 Introduction 3](#_Toc135770613)

[2.0 Patching for the vulnerability 4](#_Toc135770614)

[3.0 Step-by-step to patch the vulnerability 5](#_Toc135770615)

[3.1 Auto update method 5](#_Toc135770616)

[3.2 Manual update method 7](#_Toc135770617)

[4.0 Conclusion 12](#_Toc135770618)

[5.0 References 13](#_Toc135770619)

# Introduction

A significant issue with remote code execution has been discovered in the Internet Authentication Service (IAS) through vulnerability testing which is named MS09-071. It can be manipulated due to flaws in the MS-CHAP v2 authentication procedure and insufficient PEAP authentication request validation.

A memory corruption flaw in the PEAP authentication mechanism enables remote exploitation without authentication. Attackers can run programs with system-level rights, taking full control of the system they are targeting. Additionally, attackers can take advantage of the vulnerability and execute code remotely by providing a fake MS-CHAP v2 authentication request. They can take over a user's rights and access private information.

By taking advantage of this flaw, a remote attacker can get access and take over a specific user's rights. Microsoft has given this vulnerability a severe aggregate severity rating as its significant impact on the security of the operating system. As a result, it is essential to develop an effective technique for fixing this vulnerability, which will be covered in more detail.

# Patching for the vulnerability

In order to find possible targets, attackers frequently search for systems running out-of-date software. Updating the operating system to the latest version is crucial for addressing and patching vulnerabilities. This is because it can effectively fix the issue by making essential changes to the way the Server service processes RPC request, a protocol that enables a program to ask another program running on a different computer in a network for services, to ensure the security of the system increase and limiting any risks (BetaFred, 2008). Hence, users can prevent unauthorized access and potential vulnerability exploitation by deploying the patches and decreasing the security gap in the software.

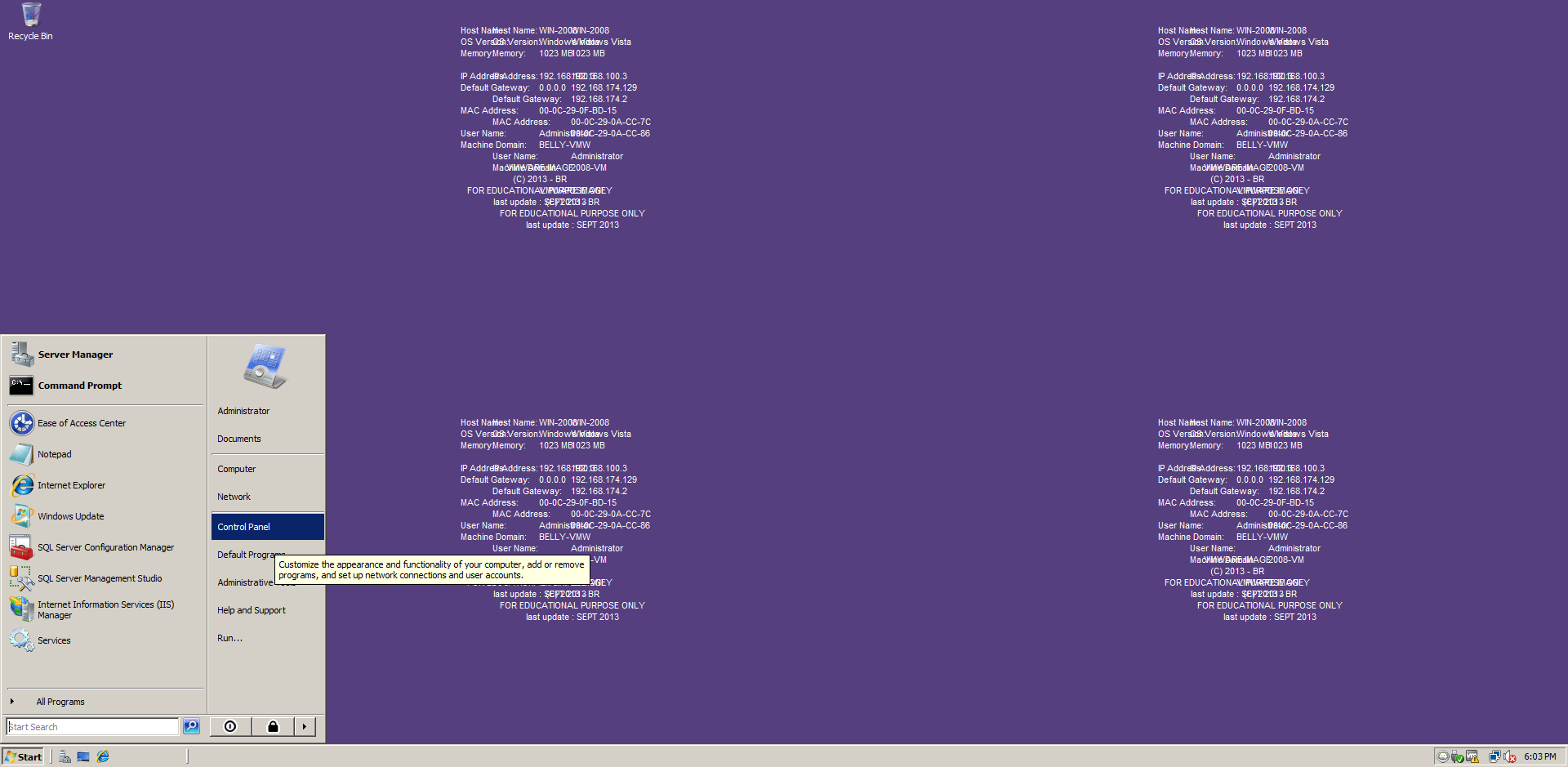
Moreover, operating system updates address more than just specific vulnerabilities, they also contain standard fixes and updates that enhance the system's general stability, performance, and compatibility (Hetler, 2022). For example, users can benefit from a compiled set of patches and improvements that bring the system up to date and running optimally.

There are two methods for updating the operating system, each with its considerations. The first method depends on the **automatic update** feature and is suitable for customers who have turned on this feature. Users can get security updates via the Microsoft Download Centre, which can be quickly found by using a keyword search for "security update”. However, users must use the second approach which they need to **manually download** the security updates and install the software update from the Microsoft Update Catalog if the automatic updating feature is disabled. Microsoft Update Catalog, which is a database that includes security updates, drivers, and service packs, is searchable and available through Microsoft Update and Windows Update (*Microsoft Update Catalog*, 2020). In the second method, users must identify their unique operating system version and architecture (x86, x64, or x32) before installing. Then, to start the update procedure, the user must find the relevant installation link by searching using the security bulletin number, such as MS09-071.

# Step-by-step to patch the vulnerability

## 3.1 Auto update method

1. Click on the control panel from the start menu.



**Figure 1: Start menu**

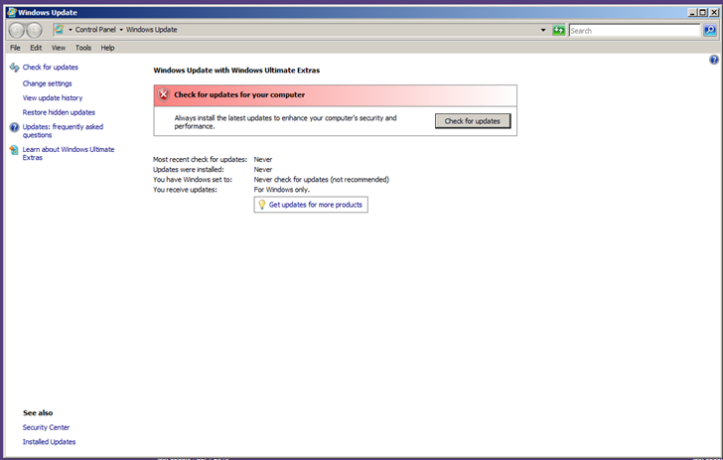
2. Control panel contains all the applications that help to change settings for things like accessibility, networking, security, hardware, and software. Clicked the window update from it.

A screenshot of a computer

Description automatically generated

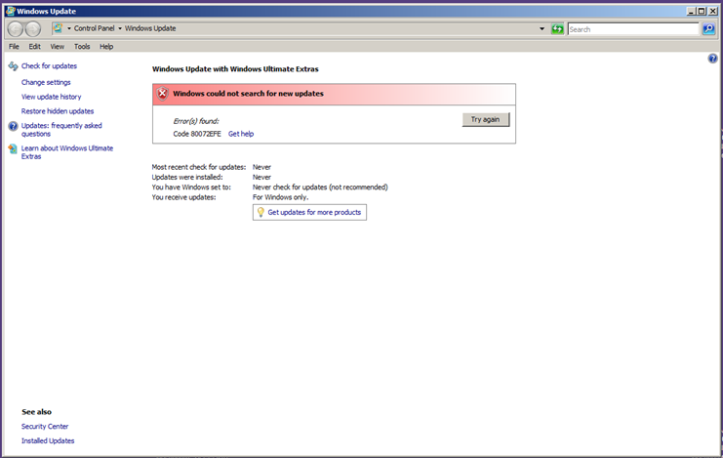
**Figure 2: Control panel**

3. Checked for the update.



**Figure 3: Windows update**

4. An error popped up which showed there are no longer any available automatic solutions to make the operating system update. Hence, users have to use the second method which required to update the system manually.



**Figure 4: Error message for Windows update**

## Manual update method

1. Open the web browser and search for Microsoft Update Catalog.

A picture containing text, font, line, software

Description automatically generated2. Click on the Microsoft Update Catalog link.

**Figure 5: Google search of Microsoft Update Catalog**

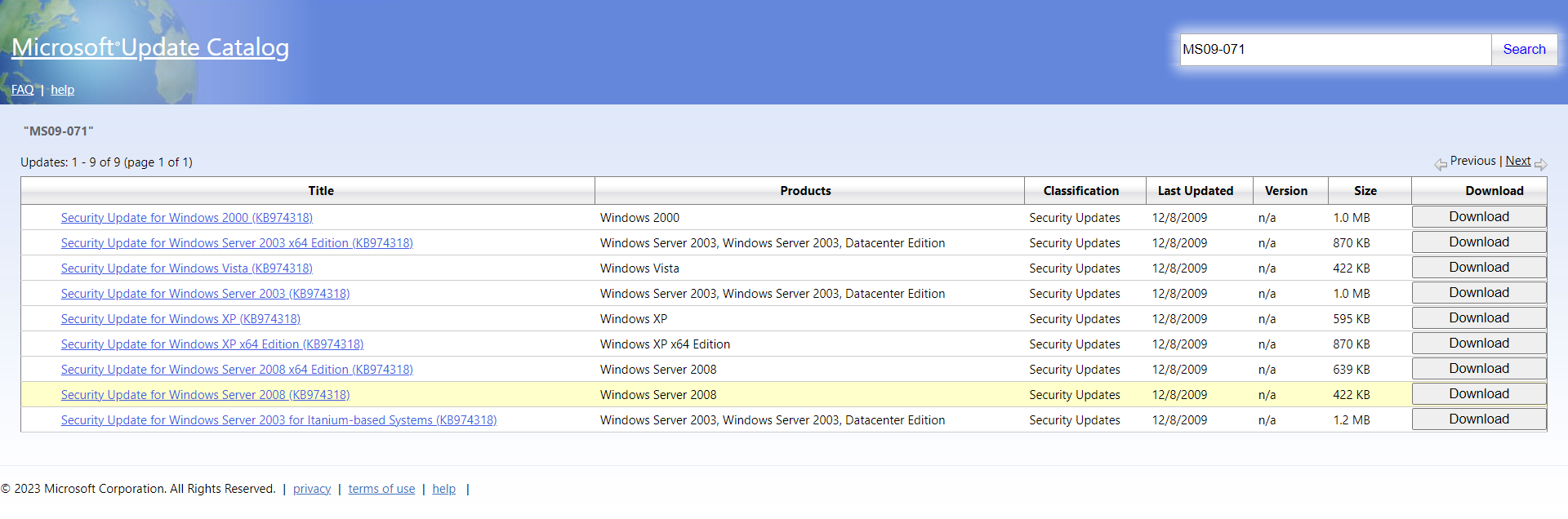
3. Search for the vulnerability which is MS09-71.

A picture containing text, software, operating system, computer icon

Description automatically generated

**Figure 6: Search for MS09-071**

4. Find the selection related to the operating system with the title. For example, I will click the "Windows Server 2008 for x32-based systems" option.

**

**Figure 7: Software selection in the Microsoft update catalog**

5. A pop-up modal will be shown on the screen. Click on the link to download the window update package.

A screenshot of a computer

Description automatically generated

**Figure 8: Pop-up modal**



**Figure 9: Downloaded Windows update package**

6. Copy the downloaded Windows update package to the external hard drive for further purposes. For this scenario, I used a USB flash drive for it.

A screenshot of a computer

Description automatically generated

**Figure 10: Move the Windows update package to the USB flash drive**

7. Connected the USB Device to the virtual machine, which is the Windows 2008.

A screenshot of a computer

Description automatically generated

**Figure 11: New USB Device Detected in Windows Server 2008**

8. Open the USB drive.

A screenshot of a computer

Description automatically generated

**Figure 12: Open USB Device**

9. Open the window update package in the file explorer.

A screenshot of a computer

Description automatically generated

**Figure 13: File explorer**

10. Clicked on the windows

A screenshot of a computer

Description automatically generated

**Figure 14: Windows update standalone installer**

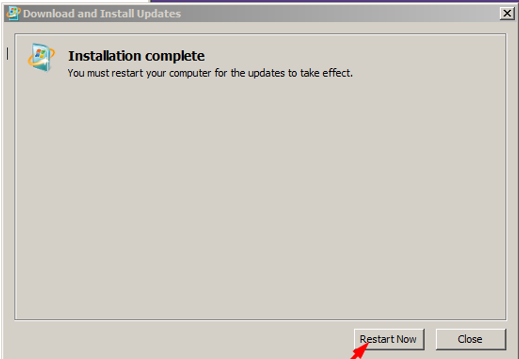
11. Select “OK” option to install the window software update

A screenshot of a computer error

Description automatically generated with low confidence

**Figure 15: Confirmation for the Windows update standalone installer**

11. After the software package is installed, the user can restart the operating system, and the software has been updated.



**Figure 19: Installation Complete**

# Conclusion

The serious vulnerability called MS09-071 allows attackers to remotely execute code on a victim's computer. This vulnerability makes use of a mistake in the Internet Authentication service, which results in improper handling of appropriate authentication requests. Both automatic updates and manual updates are options for addressing this issue. Both methods have been thoroughly described, with step-by-step directions for correctly applying the required fixes and addressing the problem. The users can make sure that their system remains protected against the threats presented by the MS09-071 vulnerability by following these guidelines.

# References

BetaFred. (2008, October 13). *Microsoft Security Bulletin MS08-067 - Critical*. Learn.microsoft.com. <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>

Hetler, A. (2022, May 18). *5 reasons software updates are important*. WhatIs.com. <https://www.techtarget.com/whatis/feature/5-reasons-software-updates-are-important#:~:text=Updates%20can%20prevent%20security%20issues%20and%20improve%20compatibility%20and%20program%20features.&text=Software%20updates%20are%20necessary%20to>

*Microsoft Update Catalog*. (2020). Microsoft.com. <https://www.catalog.update.microsoft.com/Home.aspx>