



---

In-Depth Analysis of CVE-2024-38074  
Remote Code Execution Vulnerability in Windows Remote Desktop Licensing  
Service

---

Report



PRESENTED BY: RAVEEHA NASEEM

SUBMITTED TO: SIR BILAL

AUGUST 19, 2024

**CORVIT EDUCATION SYSTEM MULTAN**

**Table of Contents**

INTRODUCTION ..... 2

- Overview of the Vulnerability: ..... 2
- Importance of the Report: ..... 2

VULNERABILITY DETAILS ..... 2

- Technical Specifications: ..... 2
- CVSS Score and Impact:..... 3

ATTACK VECTORS AND EXPLOITATION ..... 3

- How the Vulnerability Can Be Exploited: ..... 3
- Proof of Concept (PoC) and Real-World Exploits:..... 3

MITIGATION AND PATCHING..... 4

- Official Patches from Microsoft: ..... 4
- Alternative Mitigation Strategies: ..... 4

SECURITY RECOMMENDATIONS ..... 4

- Best Practices for Protecting Systems:..... 4
- Long-Term Security Considerations: ..... 4

REFERENCES AND RESOURCES..... 5

## INTRODUCTION

- **Overview of the Vulnerability:**

CVE-2024-38074 is a critical Remote Code Execution (RCE) vulnerability discovered in the Windows Remote Desktop Licensing Service. This vulnerability allows unauthenticated attackers to execute arbitrary code on the target system, leading to potential full system compromise. Given its critical nature, it has attracted significant attention in the cybersecurity community.

- **Importance of the Report:**

This report aims to provide a comprehensive understanding of the vulnerability, its technical details, potential impacts, and the necessary steps for mitigation. It is essential for IT professionals, system administrators, and security teams to be aware of and address this vulnerability to protect their systems and data.

## VULNERABILITY DETAILS

- **Technical Specifications:**

- ❖ CVE ID: CVE-2024-38074
- ❖ Type: Remote Code Execution
- ❖ CVSS Score: 9.8 (Critical)
- ❖ Attack Vector: Network
- ❖ Privileges Required: None
- ❖ User Interaction: None
- ❖ Impact: Complete control over the affected system

- **Affected Systems and Software:**

This vulnerability affects multiple versions of Windows Server, including:

- ❖ Windows Server 2008 R2 SP1
- ❖ Windows Server 2012 and 2012 R2
- ❖ Windows Server 2016
- ❖ Windows Server 2019
- ❖ Windows Server 2022

- **CVSS Score and Impact:**

The CVSS score of 9.8 reflects the severity of the vulnerability, highlighting the potential for complete system compromise if exploited. The exploit requires no privileges and can be executed remotely, increasing its risk profile.

## **ATTACK VECTORS AND EXPLOITATION**

- **How the Vulnerability Can Be Exploited:**

The vulnerability exists in the Windows Remote Desktop Licensing Service, where a flaw in the code allows attackers to execute arbitrary commands. Exploitation can be achieved remotely, without user interaction, making it an attractive target for attackers.

- **Proof of Concept (PoC) and Real-World Exploits:**

While public PoCs are limited, security researchers have demonstrated the potential for exploiting this vulnerability. In controlled environments, arbitrary code execution has been achieved, emphasizing the need for immediate action.

## MITIGATION AND PATCHING

- **Official Patches from Microsoft:**

Microsoft has released patches to address this vulnerability. It is strongly recommended that all affected systems apply these patches immediately to prevent exploitation.

- **Alternative Mitigation Strategies:**

For systems that cannot be patched immediately, implementing strict network access controls and monitoring unusual activity can help mitigate the risk. Disabling unnecessary services and ensuring that only authorized users have access to critical systems is also advisable.

## SECURITY RECOMMENDATIONS

- **Best Practices for Protecting Systems:**

- ❖ Apply patches as soon as they are available.
- ❖ Limit network exposure for systems that are critical or have known vulnerabilities.
- ❖ Regularly monitor systems for signs of unusual activity.
- ❖ Conduct regular security audits and vulnerability assessments.

- **Long-Term Security Considerations:**

In addition to addressing the immediate threat posed by CVE-2024-38074, organizations should consider long-term strategies for improving their overall security posture. This includes implementing a robust patch management process, enhancing network security measures, and investing in security training for IT staff.

## REFERENCES AND RESOURCES

[National Vulnerability Database \(NVD\) - CVE-2024-38074](#)

[Microsoft Security Response Center \(MSRC\) - CVE-2024-38074](#)

[CERT-EU Security Advisory](#)

[Bleeping Computer - Exploits Released for Critical Jenkins RCE Flaw](#)

# THE END