IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

Defend Yourself from CVE-2023-23397

Prof. Nigade S.[1], Yogita M Jadhav[2], Gautami M Badadhe[3], Saurabh G Bhokare[4], Shambhuraje U Kale[5]
Professor, Department of Computer Science and Engineering[1]
Students,DepartmentofComputerScience&Engineering[2,3,4,5]
Navsahyadri Education Society's Group of Institutions, Polytechnic, Pune, Maharashtra, India

Abstract: *The Common Vulnerabilities and Exposures (CVE) identifier CVE-2023-23397 describes a critical security flaw in Microsoft Outlook. This vulnerability allows attackers to execute privilege escalation attacks by crafting malicious calendar invites or messages, exploiting the NTLM authentication protocol without user interaction. This paper discusses the technical aspects of the vulnerability, mitigation strategies, and its broader implications for Cyber security. In addition to detailing the mechanics of CVE-2023-23397, this paper will also explore the potential impact on organizations, particularly those heavily reliant on Microsoft Outlook for communication and scheduling. The ability for attackers to leverage this vulnerability to escalate privileges poses significant risks, including unauthorized access to sensitive information and systems. By examining real-world scenarios and case studies, we will highlight the urgency of addressing this vulnerability and implementing robust security measures. Furthermore, this analysis aims to foster a deeper understanding of the importance of regular software updates, user education, and the adoption of security best practices as essential components in the defence against evolving cyber threats. Insider Security analysed the possible exploitation techniques for the recent Outlook vulnerability, as well as methods for early detection of such exploits, both for this specific vulnerability and future similar vulnerabilities. Microsoft recently released a patch for Outlook vulnerability CVE-2023-23397, which has been actively exploited for almost an entire year.*

Keywords: Arduino, IR Sensor, DC Motor, Android Studio

I. INTRODUCTION

The Common Vulnerabilities and Exposures (CVE) identifier CVE-2023-23397 describes a critical security flaw in Microsoft Outlook. This vulnerability allows attackers to execute privilege escalation attacks by crafting malicious calendar invites or messages, exploiting the NTLM authentication protocol without user interaction. This paper discusses the technical aspects of the vulnerability, mitigation strategies, and its broader implications for Cyber security.In addition to detailing the mechanics of CVE-2023-23397, this paper will also explore the potential impact on organizations, particularly those heavily reliant on Microsoft Outlook for communication and scheduling. The ability for attackers to leverage this vulnerability to escalate privileges poses significant risks, including unauthorized access to sensitive information and systems. By examining real-world scenarios and case studies, we will highlight the urgency of addressing this vulnerability and implementing robust security measures. Furthermore, this analysis aims to foster a deeper understanding of the importance of regular software updates, user education, and the adoption of security best practices as essential components in the defence against evolving cyber threats. A serious vulnerability tagged CVE-2023-23397 has recently been released to the public after CERT-UA warned the cyber community that has been utilizing Microsoft Outlook. The current exploit is not an isolated incident, but rather part of a series of similar vulnerabilities that go back to 2017. Some of these vulnerabilities, including CVE-2017-8572 and CVE-2017-11927, have enabled hackers to obtain a user's NTLMv2 credentials from Outlook in the past as well. What makes the issue much more critical is the fact that it doesn't require any action from the user to be activated

DOI: 10.48175/IJARSCT-25256

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

II. LITERATURE REVIEW

- NTLM Authentication Protocol NTLM, a widely-used authentication protocol, has been historically exploited in various attacks, such as Pass-the-Hash. Research shows inherent weaknesses in NTLM, particularly its inability to effectively mitigate relay attacks.
- Microsoft Outlook Vulnerabilities Studies reveal that email platforms like Outlook are attractive targets due to their integration with organizational systems. Previous vulnerabilities, including privilege escalation attacks, highlight the need for robust security.
- Defence Techniques Against Credential Theft Several studies have proposed techniques to mitigate credential theft, including multifactor authentication (MFA), blocking external NTLM traffic, and implementing robust email filtering. Enhancing NTLM Security Measures To address the inherent weaknesses of the NTLM authentication protocol, organizations can adopt several best practices aimed at strengthening their security posture. One effective strategy involves migrating to more secure authentication protocols, such as Kerberos, which provides better defence against attacks like Pass-the-Hash and relay attacks. Additionally, restricting NTLM usage within the network, through group policies or security settings, can significantly reduce the attack surface. Regular audits and assessments of NTLM configurations and authentications can help identify potential vulnerabilities and enforce compliance with security policies.
- Current Landscape of Email Security Threats Given the critical role of email in modern business operations, ongoing vigilance against vulnerabilities in platforms like Microsoft Outlook is vital. Attackers are increasingly exploiting email-related functionalities, leveraging advanced social engineering tactics to deceive users into inadvertently granting access to sensitive data. Awareness campaigns and training programs are essential in educating employees about recognizing phishing attempts and understanding the signs of potential threats. Moreover, integration of threat intelligence services can assist organizations in staying abreast of emerging vulnerabilities and attacks, enabling prompt responses.
- Implementing Layered Security Approaches The implementation of a layered security strategy is paramount in protecting against credential theft and other related threats. In addition to multifactor authentication (MFA) and enhanced email filtering, organizations should consider adopting endpoint detection and response (EDR) solutions that continuously monitor and analyze behaviour on devices to detect anomalies. Network segmentation, along with strict access controls based on the principle of least privilege, can limit the potential impact of credential theft. Furthermore, regular software patching and updates are critical to ensuring that any known vulnerabilities, including those within the NTLM protocol and email systems, are promptly addressed, thereby reducing the window of opportunity for attackers.

III. OBJECTIVE

1. Analyze CVE-2023-23397, its exploit mechanism, and its impact.
2. Propose mitigation strategies to safeguard systems from exploitation.
3. Offer practical applications to enhance Cyber security in organizational environments.

Importance: With organizations increasingly relying on digital communication platforms, the exploitation of vulnerabilities like CVE-2023-23397 can lead to devastating data breaches and financial losses

IV. TECHNOLOGY

Due to hardware project we use rasberry pi pico chip

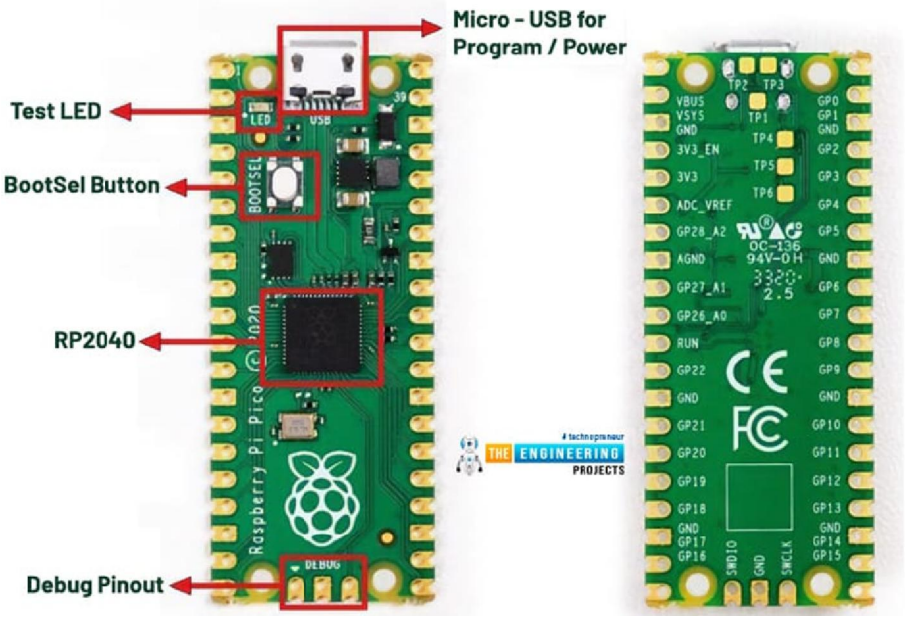
HARDWARE DESCRIPTION

The Raspberry Pi Pico is a small, affordable microcontroller board powered by the RP2040 chip, a custom-designed chip from Raspberry Pi. It features a dual-core ARM Cortex-M0+ processor, 264 KB of SRAM, and 2 MB of on-board QSPI flash memory. The Pico can be programmed in C and MicroPython and is often used for IoT projects and other physical computing applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

RP2040 Chip Details:
Processor: Dual-core ARM Cortex-M0+ processor.
Frequency: Up to 133 MHz.
RAM: 264 KB on-chip SRAM.
Flash: 2 MB on-board QSPI flash memory.
I/O: 26 GPIO pins, including 3 analog inputs.
Interfacing: 2 x SPI, 2 x I2C, 2 x UART, 3 x 12-bit ADC, 16 x controllable PWM channels.
USB: Includes USB 1.1 device and host support for drag-and-drop programming.

V. SYSTEM ARCHITECTURE DIAGRAM



VI. MAJOR FIELD APPLICATION

1. Enterprise Security: Mitigating vulnerabilities in organizational email systems to protect sensitive information.
2. Government Systems: Enhancing Cyber security for government communication platforms.
3. Healthcare: Protecting patient data in healthcare organizations.
4. Finance: Ensuring secure financial transactions and correspondence.
5. Education Sector: Safeguarding Student and Institutional Data
6. Utilize secure email platforms for safe communication, implement email encryption to protect sensitive data, and conduct user awareness training focused on identifying phishing attacks.
7. Retail and E-Commerce: Securing Customer Payment Information 8. Employ end-to-end email encryption, enforce access control measures to limit data exposure, and ensure compliance with PCI DSS to protect customer payment information. 9. Manufacturing: Protecting Intellectual Property and Supply Chain Information 10. Implement strong Cyber security measures like multi-factor authentication and data loss prevention, use secure file-sharing systems, and safeguard against intellectual property theft.

VII. ADVANTAGES ANDAPPLICATIONS

7.1 ADVANTAGES

- Patching
- Protected Users Group

DOI: 10.48175/IJARSCT-25256

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

• Blocking TCP 445/SMB Outbound
• Enforce SMB Signing

7.2 APPLICATION

• Deploying Patches: Install security updates released by Microsoft for Outlook.
• Enforcing Email Filtering: Block suspicious attachments and calendar invites at the server level.
• Disabling NTLM Authentication: Configure systems to disable external NTLM traffic, reducing the attack surface.
• Employee Training: Educate employees on recognizing malicious emails and calendar invites

VIII. CONCLUSIONANDFUTURESCOPE

CVE-2023-23397 demonstrates the evolving threat landscape in Cyber security. By exploiting the NTLM protocol, attackers can compromise user credentials and gain unauthorized access. Implementing robust defence mechanisms, including patch management, network configuration, and user education, is vital for mitigating such vulnerabilities. Future efforts should focus on advancing authentication protocols and real-time detection mechanisms to prevent similar threats

• Enhanced Authentication Protocols
• AI-based Threat Detection
• Global Cyber security Standards
• Multi-Factor Authentication (MFA)

REFERENCES

[1]. Microsoft Security Updates. (2023). Security Advisory for CVE-2023-23397. Retrieved from [Microsoft.com]
[2]. Smith, J., & Brown, K. (2021). Analysis of NTLM Vulnerabilities in Modern Systems. CyberSec Journal. •
[3]. National Institute of Standards and Technology (NIST). (2023). Vulnerability Database Entry for CVE-2023-23397