CORVIT
Reaching end to end

Corvit systems Multan

Course: CEH(Certified Ethical Hacking)

Assignment#4

CVE-2024-38173

Microsoft Outlook Remote Code Execution Vulnerability

Submitted by: Hasnain Raza

Submitted to: Muhammad Bilal

Date: 19-08-2024

CVE-2024-38173: **Microsoft Outlook Remote Code Execution Vulnerability**

Introduction

CVE-2024-38173 is a severe Remote Code Execution (RCE) vulnerability discovered in Microsoft Outlook. This zero-click vulnerability allows attackers to execute arbitrary code on a target system simply by sending a malicious email, without requiring any user interaction.

Vulnerability Details

- **Type:** Remote Code Execution (RCE)
- **CVSS score:** 6.7
- **Severity:** Medium (6.7)
- **Impact:** Potential data breaches, unauthorized access, and other malicious activities.
- **Exploitation:** Zero-click, no user interaction required if auto-open email is enabled.
- **Affected Software:** Microsoft Outlook, Office 2019,Microsoft 365
- **Disclosure Date:** June 16, 2024
- **Patch Released:** August 2024 Patch Tuesday

Technical Impact

This vulnerability arises from a flaw in Outlook's handling of form injection. By crafting a malicious email with a specially designed form, an attacker can execute arbitrary code on the victim's system. The zero-click nature of this vulnerability makes it particularly dangerous, as users are unaware of the threat.

Potential Consequences

Successful exploitation of CVE-2024-38173 could lead to catastrophic consequences, including:

- **Data theft:** Attackers can steal sensitive information, such as personal data, financial records, and intellectual property.
- **System takeover:** Complete control of the compromised system, allowing attackers to install malware, deploy ransomware, or use the system for further malicious activities.
- **Lateral movement:** Attackers can leverage the compromised system as a foothold to spread to other systems within a network.

Mitigation Steps

To protect against CVE-2024-38173, it is crucial to implement the following measures:

- **Apply the latest patches:** Install the August 2024 Patch Tuesday updates from Microsoft to address this vulnerability.
- **Email security best practices:** Implement robust email security measures, including spam filters, antivirus software, and user education about phishing attacks.
- **Network segmentation:** Isolate sensitive systems and networks to limit the potential impact of a successful attack.
- **Incident response plan:** Develop a comprehensive incident response plan to effectively handle a security breach.

Additional Considerations

While the patch for CVE-2024-38173 has been released, it's essential to remain vigilant. New vulnerabilities may emerge, and attackers might find ways to bypass existing protections. Keeping software up-to-date, practicing good security hygiene, and staying informed about the latest threats are crucial for maintaining a strong security posture.

Conclusion

CVE-2024-38173 highlights the ongoing challenge of securing email environments. The zero-click nature of this vulnerability underscores the importance of proactive security measures. By promptly applying patches, implementing email security best practices, and staying informed about emerging threats, organizations can significantly reduce the risk of successful attacks.