NCA-28.051625 – National CERT Advisory – Important Local Remote Code Execution Vulnerability in Microsoft Outlook (CVE-2025-32705)

Introduction

An important remote code execution (RCE) vulneraility, CVE-2025-32705 (CVSS 7.8), has been identified in Microsoft Outlook, affecting multiple editions of Microsoft Outlook including Office LTSC 2021, Office LTSC 2024, and Microsoft 365 Apps (32-bit and 64-bit). This vulnerability was patched as part of Microsoft's May 2025 Patch Tuesday.

CVE-2025-32705 is classified as a Remote Code Execution (RCE) vulnerability, with a CVSS v3.1 base score of 7.8 (Important). It arises from an out-of-bounds memory read flaw in the Outlook application, which, under certain conditions, allows attackers to execute arbitrary code locally on the victim's machine after a user opens a maliciously crafted file.

Although exploitation requires user interaction, such as opening an infected attachment, the potential for local code execution, privilege escalation, and system compromise renders this vulnerability a serious threat—especially in enterprise environments where Outlook is widely deployed.

Impact

If successfully exploited, CVE-2025-32705 can lead to:

1. **Arbitrary Code Execution** – Execution of attacker-controlled code on the local system.
2. **Privilege Abuse** – The attack executes in the context of the current user, potentially escalating depending on privilege levels.
3. **Lateral Movement** – Post-exploitation activities may allow attackers to move laterally across networks.
4. **Data Exposure and Theft** – Unauthorized access to local files, cached credentials, and email data.
5. **Malware or Ransomware Deployment** – The flaw may be used as an initial vector for broader system compromise.

While the vulnerability is not currently known to be actively exploited in the wild, its exploitability via user interaction and potential system impact underscore the urgency for mitigation.

Threat Details

Vulnerability Overview

- **CVE ID**: CVE-2025-32705
- **Component Affected**: Microsoft Outlook
- **Vulnerable Products**:

    - Microsoft Office LTSC 2021 (32-bit and 64-bit)
    - Microsoft Office LTSC 2024 (32-bit and 64-bit)
    - Microsoft 365 Apps for Enterprise (32-bit and 64-bit)
- **Vulnerability Type**: Out-of-Bounds Read → Local Code Execution
- **Attack Vector**: Local (requires user to open a malicious file)
- **Attack Complexity**: Low
- **Privileges Required**: None (runs in context of user)
- **User Interaction**: Required
- **CVSS v3.1 Score**: 7.8 (Important)
- **CWE ID**: CWE-125 – Out-of-Bounds Read

Technical Description

This vulnerability results from a flaw in memory boundary checking within Microsoft Outlook's file handling mechanism. When a specially crafted file (likely an email attachment or external file) is opened in an unpatched Outlook instance, it triggers an out-of-bounds read condition. This can cause memory corruption, potentially enabling the attacker to execute arbitrary code in the context of the user.

Importantly, this vulnerability cannot be exploited via the Outlook Preview Pane, mitigating risk from passive viewing. However, active engagement by the user (i.e., opening the malicious file) is required, making this a locally triggered remote code execution vulnerability.

Exploit Conditions

For CVE-2025-32705 to be exploited, the following conditions must be present:

- The user is operating an affected version of Microsoft Outlook.
- The user receives a malicious file, often through phishing or drive-by downloads.
- The user actively opens the file using Microsoft Outlook.
- The system has not yet applied the security update released in May 2025.

While exploitation complexity is considered low, effective delivery and user interaction make it a favored vector in targeted spear-phishing campaigns.

Affected Systems & Required Updates

Product	Impacted Versions	Fixed Version / Patch Action
Microsoft Office LTSC 2021	32-bit, 64-bit	Apply May 2025 Outlook Security Update
Microsoft Office LTSC 2024	32-bit, 64-bit	Apply May 2025 Outlook Security Update
Microsoft 365 Apps for Enterprise	32-bit, 64-bit	Apply May 2025 Outlook Security Update

Microsoft has published specific guidance and download links through its Security Update Guide.

Recommendations & Mitigation Actions

1. Apply Security Patches Immediately

- Organizations must deploy the official Microsoft updates released on May 14, 2025, to all vulnerable Outlook installations.
- This is the most effective mitigation against exploitation.

2. Restrict File Handling Behavior

- Consider enforcing Group Policy Objects (GPOs) or endpoint control policies that limit execution or opening of untrusted files in Outlook.

3. User Awareness and Email Hygiene

- Conduct security awareness training focusing on:
  - Avoiding unsolicited attachments.
  - Reporting suspicious emails or files.
  - Recognizing social engineering tactics.

4. Enhance Endpoint and Network Security

- Ensure antivirus, EDR, and firewall tools are updated to detect exploitation patterns.
- Use sandboxing and email filtering to inspect attachments before delivery.

5. Monitoring and Detection

- Monitor logs for:
  - Unexpected Outlook process activity.
  - Attempts to access unusual memory regions.
  - File launches from email directories (e.g., %TEMP%, %APPDATA%).

6. Email Gateway Defense

- Utilize **email security gateways** that:
  - Scan attachments for known exploits or abnormal file structures.
  - Strip or quarantine suspicious content.

Incident Response & Preparedness

- Review and test incident response plans to include Outlook-based RCE events.

- Regularly back up user data, ensuring offline storage copies to reduce ransomware risks.
- Validate that endpoint rollback or isolation procedures are functioning.

Patching Summary

Product	Version Range	Status	Action
All Affected Outlook Builds	As listed	Vulnerable	Apply May 2025 Outlook Patch
Patched Versions	Post-May 2025	Secure	No action required beyond patching

References

1. NVD CVE-2025-32705
2. Tenable Advisory – CVE-2025-32705
3. Microsoft MSRC Security Advisory

Call to Action

The National CERT strongly urges all government organizations, enterprises, and individuals using Microsoft Outlook to:

- Apply all available patches released in the May 2025 Patch Tuesday rollout without delay.
- Implement email filtering, segmentation, and endpoint controls to reduce attack surface.
- Increase user vigilance through awareness campaigns and simulated phishing exercises.
- Monitor official vendor advisories and vulnerability databases to remain informed of evolving threats.

Proactive patching, user education, and layered security remain essential to reducing exposure to email-borne vulnerabilities and protecting against modern code execution threats.