NCA-16.041025 – NCERT Advisory – WhatsApp Desktop for Windows File Attachment Spoofing Vulnerability (CVE-2025-30401)

Introduction

A high-severity security vulnerability has been discovered in WhatsApp Desktop for Windows, a widely used instant messaging platform in both personal and enterprise environments. The flaw, tracked as CVE-2025-30401, enables remote attackers to trick users into executing malicious code via spoofed file attachments.

This vulnerability arises due to a discrepancy between MIME type rendering and file extension handling, where WhatsApp displays attachments based on their MIME type but opens them using the file extension defined in the operating system. This logic flaw can be exploited by an attacker to disguise an executable file (e.g., .exe) as a benign file (e.g., .jpg), leading to arbitrary code execution when the user opens the file within WhatsApp.

WhatsApp versions prior to 2.2450.6 for Windows are affected. Meta, the parent company of WhatsApp, has released a patch to remediate this vulnerability. Immediate action is advised to minimize the risk of compromise.

Impact

Successful exploitation of this vulnerability can result in:

1. **Arbitrary Code Execution** – Execution of attacker-controlled code through deceptive file attachments.
2. **Unauthorized Access** – Attackers may gain access to sensitive system functions or data.
3. **Privilege Abuse** – Malicious code could operate with user-level privileges or attempt elevation.
4. **Group-Based Exploitation** – Malicious files shared in group chats can target multiple users at once.
5. **Security Bypass** – Traditional attachment scanning and file previews may be bypassed.

Vulnerability Details

The vulnerability is due to WhatsApp's inconsistent processing of file attachments:

- The application displays files using the MIME type, suggesting a safe file format (e.g., an image).

- However, it executes the file using the system's file extension, which may be malicious (e.g., .exe).

This mismatch enables attackers to craft spoofed attachments that appear harmless but execute dangerous payloads when opened.

CVE-2025-30401 – A spoofing issue in WhatsApp Desktop for Windows versions prior to 2.2450.6, where a maliciously crafted mismatch between MIME type and file extension could lead to arbitrary code execution when a user opens an attachment directly within the app.

Affected Systems

The following versions of WhatsApp Desktop for Windows are impacted by this vulnerability:

- Versions from 0.0.0 up to, but not including, 2.2450.6

Systems running these versions, especially those used for file sharing or communication in sensitive environments, are at risk if the application is not updated.

Recommendations & Action Items

1. Immediate Mitigation Measures

a. Update to Patched Version

- Upgrade WhatsApp Desktop for Windows to **version 2.2450.6 or higher**.
- Updates are available via the official WhatsApp website or the Microsoft Store.

b. Restrict File Handling Practices

- Avoid opening attachments directly within WhatsApp, especially files with **double extensions** (e.g., .jpg.exe).
- Encourage users to **verify file extensions** and **scan files with antivirus tools** before opening.

c. Show File Extensions

- Configure Windows File Explorer to display full file extensions to prevent extension spoofing.

2. Endpoint Protection & Access Controls

a. Deploy Antivirus and EDR Tools

- Ensure real-time protection is enabled on all endpoints.

- Use endpoint detection and response (EDR) solutions to monitor suspicious file execution.

b. Harden Workstation Policies

- Prevent execution of unknown file types in user directories (Downloads, Temp).
- Enforce policies that restrict launching of executable files received through messaging platforms.

3. Monitoring & Logging

- Monitor system logs for processes initiated by WhatsApp involving suspicious file types.
- Use SIEM tools to correlate activity patterns across endpoints, especially where file attachments are received and executed.

4. User Awareness and Education

- Conduct awareness campaigns about **file spoofing attacks**.
- Aware users to recognize suspicious attachments and practice safe file handling.

Patching & Updates

Meta has released the following updated version to address CVE-2025-30401:

Affected Version Range	**Secure Version**
WhatsApp Desktop ≤ 2.2450.5	**Update to 2.2450.6 or later**

All organizations and users are strongly advised to apply this update immediately.

Strengthen Security Posture

- Segment messaging applications from core business infrastructure.
- Apply least privilege principles to limit execution rights on user systems.
- Use application control and whitelisting to restrict unapproved software execution.

Disaster Recovery & Incident Readiness

- Maintain secure, encrypted backups of critical data and configurations.

- Review and test incident response plans for social engineering and remote code execution scenarios.
- Regularly assess messaging platforms for vulnerabilities and misconfigurations.

References

1. **CVE Details – CVE-2025-30401:** https://nvd.nist.gov/vuln/detail/CVE-2025-30401
2. **WhatsApp Version History:** https://www.whatsapp.com/download
3. **MITRE CVE Entry:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-30401

Call to Action

The National CERT strongly urges all users and organizations using WhatsApp Desktop for Windows to:

- Apply the latest patch (v2.2450.6 or higher),
- Educate end users on spoofed file risks,
- Enforce strong endpoint controls, and
- Monitor for unusual file execution behaviors.

Preventive action and secure handling of messaging applications are critical to safeguarding personal and organizational systems from this vulnerability.