Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 331 **06-09-2024**

Name: New Flaws in Microsoft macOS Apps Could Allow Hackers to Gain Unrestricted Access

Threat Classification: Privilege Escalation / Code Injection

Affected Software / Services:

- **Operating System:** macOS
- **Microsoft Applications for macOS:**
  - Outlook
  - Teams (specific versions patched as of the latest update)
  - Word
  - Excel
  - PowerPoint
  - OneNote (specific versions patched as of the latest update)

Summary:

Eight vulnerabilities have been identified in various Microsoft applications for macOS, including Outlook, Teams, Word, Excel, PowerPoint, and OneNote. These vulnerabilities could allow an attacker to exploit the permissions granted to these applications to gain unauthorized access to sensitive data or perform privileged actions without user consent. The vulnerabilities enable the injection of malicious libraries, which inherit the applications' permissions, circumventing the TCC framework and macOS security measures. Microsoft has patched some of these vulnerabilities in recent updates to Teams and OneNote.

Severity	High
Attack Vector	Local privilege escalation via library injection (Dylib Hijacking)

Recommendations:

- Ensure that all Microsoft applications for macOS are updated to the latest versions and patches. Further details and patch links can be found on the official websites of Microsoft and Cisco Talos.
    - Microsoft Update Catalog
- Additionally, updating your macOS to the latest version, which may include security improvements and patches, is recommended. You can update macOS from the Apple menu by selecting **System Preferences > Software Update.**
- Regularly review and limit the permissions granted to applications, particularly those that have access to sensitive data.
- Set up monitoring and alerting mechanisms for suspicious behavior such as unauthorized application activities.
- Enforce hardened runtime and library validation settings to minimize the risk of unauthorized code execution.
- Educate users on the risks associated with privilege escalation and ensure they only install trusted software and plugins.
- In case of any incident, please report to this office, through PTA CERT Portal and email.