Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 257 **09-05-2024**

Name: Adobe Acrobat and Adobe Reader Use-After-Free Vulnerability

Threat Classification: Vulnerability in Adobe Acrobat and Adobe Reader

Affected Software / Services:

- Adobe Acrobat Reader

Summary:

Adobe Acrobat and Adobe Reader are affected by a critical vulnerability, identified as **CVE-2024-30304**, which could allow remote attackers to execute arbitrary code on the system. This vulnerability is caused by a use-after-free error. Attackers can exploit this vulnerability by persuading a victim to open a specially crafted document, leading to the execution of arbitrary code on the system with the privileges of the victim or causing the application to crash.

Severity	**High**
Attack Vector	Code Execution

Recommendations:

- Refer to the Adobe Security Advisory for the appropriate patches (https://helpx.adobe.com/security/products/acrobat/apsb24-07.html), upgrades, or suggested workarounds to mitigate this vulnerability. Apply these updates as soon as possible to protect against potential exploitation.
- Exercise caution when opening documents from untrusted or unknown sources, especially those received via email or downloaded from the internet. Verify the legitimacy of the document and sender before opening.
- Deploy and maintain up-to-date antivirus and endpoint security solutions that can help detect and block malicious documents or code attempting to exploit this vulnerability.
- Educate users about the risks associated with opening suspicious documents and encourage them to report any unusual or suspicious activity to IT or security personnel.
- Consider enabling security features such as Protected View and Enhanced Security Settings in Adobe Acrobat and Adobe Reader to help mitigate the impact of potential exploits.
- Monitor network traffic and system logs for any signs of exploitation or unusual activity that may indicate an attempted attack targeting this vulnerability.
- In case of any incident, please report to this office, through PTA CERT Portal and email.