ARBITRARY CODE EXECUTION AND MEMORY LEAK IN ADOBE PRODUCTS

Vairav CVE Report

Date: March 12th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Multiple vulnerabilities, including **CVE-2025-27174, CVE-2025-27158, CVE-2025-27159, CVE-2025-27160, CVE-2025-27161, CVE-2025-27162, CVE-2025-24431, CVE-2025-27163**, and **CVE-2025-27164**, have been identified in Adobe Acrobat and Reader. The most severe of these vulnerabilities allows arbitrary code execution, with a **CVSS score of 7.8** (High). If exploited, these vulnerabilities could lead to system compromise and data exposure.

VULNERABILITY DETAILS

CVE-2025-27174, CVE-2025-27159, CVE-2025-27160

- **Description:** A Use After Free vulnerability in Acrobat Reader that could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction, such as opening a malicious file.
- **Impact:** Potential for arbitrary code execution leading to system compromise.
- **CVSS Score:** 7.8 (High)

CVE-2025-27158, CVE-2025-27162

- **Description:** Access of Uninitialized Pointer vulnerability in Acrobat Reader potentially leading to arbitrary code execution.
- **Impact:** Could allow an attacker to execute arbitrary code in the context of the current user.
- **CVSS Score:** 7.8 (High)

CVE-2025-27161

- **Description:** Out-of-bounds Read vulnerability in Acrobat Reader potentially leading to arbitrary code execution through a crafted file, which could result in a read past the end of an allocated memory structure
- **Impact:** Could allow an attacker to execute arbitrary code in the context of the current user.
- **CVSS Score:** 7.8 (High)

CVE-2025-24431, CVE-2025-27163, CVE-2025-27164

- **Description:** Out-of-bounds Read vulnerability in Acrobat Reader potentially leading to disclosure of sensitive memory. It requires user interaction in that a victim must open a malicious file.
- **Impact:** Could allow an attacker to bypass mitigations such as ASLR which randomizes addresses of processes and libraries in memory to prevent exploitation.
- **CVSS Score:** 5.5 (Medium)

AFFECTED VERSIONS

- Adobe Acrobat DC version 25.001.20428 and earlier.
- Adobe Acrobat Reader DC version 25.001.20428 and earlier.
- Adobe Acrobat 2024 version 24.001.30225 and earlier.
- Adobe Acrobat 2020 version 20.005.30748 and earlier.
- Adobe Acrobat Reader 2020 version 20.005.30748 and earlier.

EXPLOIT DETAILS

These vulnerabilities particularly concern environments where Adobe Acrobat and Reader are used to view, create, print, and manage PDF files on desktop and mobile platforms. Exploitation requires user interaction, such as opening a malicious file, which could lead to arbitrary code execution in the context of the current user and disclosure of sensitive memory. This could result in system compromise, data exposure, and service disruption.

RECOMMENDED ACTIONS

Patch & Upgrade to the following versions**:**

- Adobe Acrobat DC version 25.001.20432
- Adobe Acrobat Reader DC version 25.001.20432
- Adobe Acrobat 2024 version 24.001.30235
- Adobe Acrobat 2020 version 20.005.30763
- Adobe Acrobat Reader 2020 20.005.30763

ADDITIONAL SECURITY MEASURES

- **User Training**: Educate users on the risks of opening unsolicited or unexpected files, especially from unknown sources.
- **Application Hardening**: Implement application whitelisting to prevent unauthorized applications from executing.
- **Intrusion Detection Systems**: Deploy intrusion detection and prevention systems to monitor and block exploit attempts.

REFERENCES

- https://helpx.adobe.com/security/products/acrobat/apsb25-14.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com