June 11, 2026, **CYBERSECURITY**

Topic: Multiple Vulnerabilities in Adobe Acrobat Reader DC

Overview:

In its security bulletins dated April 12 and April 14, 2026, Adobe has released a security update for Adobe Acrobat and Reader for Windows and macOS. This update addresses critical and important vulnerabilities:

- Security update available for Adobe Acrobat Reader - APSB26-43 – 12/04/2026 *https://helpx.adobe.com/security/products/acrobat/apsb26-43.html*
- Security update available for Adobe Acrobat Reader - APSB26-44 – 14/04/2026 *https://helpx.adobe.com/security/products/acrobat/apsb26-44.html*

Additionally, in its security bulletin dated June 09, 2026, Adobe has also released a security update for the same product. This update addresses important vulnerabilities:

- Security update available for Adobe Acrobat Reader - APSB26-63 – 09/06/2026 *https://helpx.adobe.com/security/products/acrobat/apsb26-63.html*

Arabelle Solutions has identified several products that include an impacted version, listed below:

Affected Versions:

- prior to **26.001.21662**

Impacted Products:

- DCS and Unit Control Alspa products (C10, RTDS, HMI, Historian & CCAD)
- Mark Vie OT Armor
- Mark Vie TPCS projects (EWS, OWS & GTW)

Identified risks:

CVE-2026-34621 (CVSS V3 Score: 8,6) is a critical prototype pollution vulnerability in Adobe Acrobat Reader that can be exploited via a malicious PDF to achieve arbitrary code execution in the context of the current user, and it has been observed being actively exploited in the wild.

CVE-2026-34622 (CVSS V3 Score:8,6) is a prototype pollution vulnerability in Adobe Acrobat Reader that may allow a remote attacker to execute arbitrary code if a specially crafted file is opened, posing a high security risk although no active exploitation was reported at disclosure time.

CVE-2026-47911 (CVSS V3 Score: 7,8) is a memory corruption vulnerability that may allow arbitrary code execution when a user opens a specially crafted malicious PDF file, posing a significant security risk to the affected system.

CVE-2026-47912 to **CVE-2026-47921** (CVSS V3 Score: 7,8) are a series of memory management vulnerabilities that could allow an attacker to trigger arbitrary code execution if a victim opens a malicious PDF document, which increases the overall risk because several similar weaknesses are present.

CVE-2026-47955 (CVSS V3 Score: 7,8) is a vulnerability that may lead to arbitrary code execution after opening a crafted file, with potentially high impact on the integrity and security of the user's system.

CVE-2026-47959 (CVSS V3 Score: 7,8) is a stack overflow vulnerability that can be exploited through a malicious document to achieve arbitrary code execution in the context of the current user.

CVE-2026-47952 (CVSS V3 Score: 7,8) is a memory corruption vulnerability that may allow arbitrary code execution or cause the application to crash when processing a specially crafted file.

CVE-2026-47937 (CVSS V3 Score: 7,8) is a vulnerability related to the loading of malicious libraries, which could enable arbitrary code execution and potentially lead to privilege escalation if successfully exploited.

Mitigation:

Adobe has not provided any mitigation or workaround for this vulnerability.

Compensating control:

As a temporary compensating control, customers must not open PDF files using affected versions of Adobe Acrobat Reader unless the PDF file originates from a trusted and authenticated and expected source.

There is no reliable method to conclusively verify that a PDF file is free of malicious content prior to opening it. Consequently, PDF files from unknown, unexpected, or unverifiable sources shall be treated as untrusted and must not be opened, as doing so may result in successful exploitation of the identified vulnerabilities.

Remediation:

Upgrading the affected product to a fixed version resolves the identified vulnerabilities:

Product	Fixed Version
Acrobat Reader DC	26.001.21662 and later

Defense-in-depth:

To minimize the risk of the exploitation of current and future system vulnerabilities, Arabelle Solutions highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your Arabelle Solutions Automation & Controls Sales person or our Help Desk at +33 1 60 10 01 30 / helpdesk-control-systems@arabellesolutions.com for help with ordering cybersecurity services and solutions.

Revision History

Version	Release Date	Purpose
A	May 07, 2026	Initial version
B	June 11, 2026	Update after Adobe APSB26-63 bulletin publication