



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Adobe Acrobat Reader and Adobe Acrobat
Tracking #:432318767
Date:11-04-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Adobe has released a Priority 1 (Critical) security update addressing a high-impact vulnerability (CVE-2026-34621) affecting Acrobat and Reader on Windows and macOS.

TECHNICAL DETAILS:

Adobe has released a Priority 1 (Critical) security update addressing a high-impact vulnerability (CVE-2026-34621) affecting Acrobat and Reader on Windows and macOS.

This flaw is actively exploited in the wild, significantly increasing risk exposure. Successful exploitation enables arbitrary code execution, potentially allowing attackers to fully compromise affected systems.

Vulnerability Overview

- CVE ID: CVE-2026-34621
- Type: Prototype Pollution (CWE-1321)
- Severity: **Critical** (CVSS 9.6)
- **Exploitation Status: Confirmed active exploitation**
- Attack Vector: Remote (via malicious PDF)
- Impact: Full system compromise

Affected Products & Versions

- Acrobat DC (Continuous): ≤ 26.001.21367
- Acrobat Reader DC (Continuous): ≤ 26.001.21367
- Acrobat 2024 (Classic): ≤ 24.001.30356

Patched Versions

- Acrobat DC / Reader DC: 26.001.21411
- Acrobat 2024:
 - Windows: 24.001.30362
 - macOS: 24.001.30360

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update immediately to patched versions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://helpx.adobe.com/security/products/acrobat/apsb26-43.html>