Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

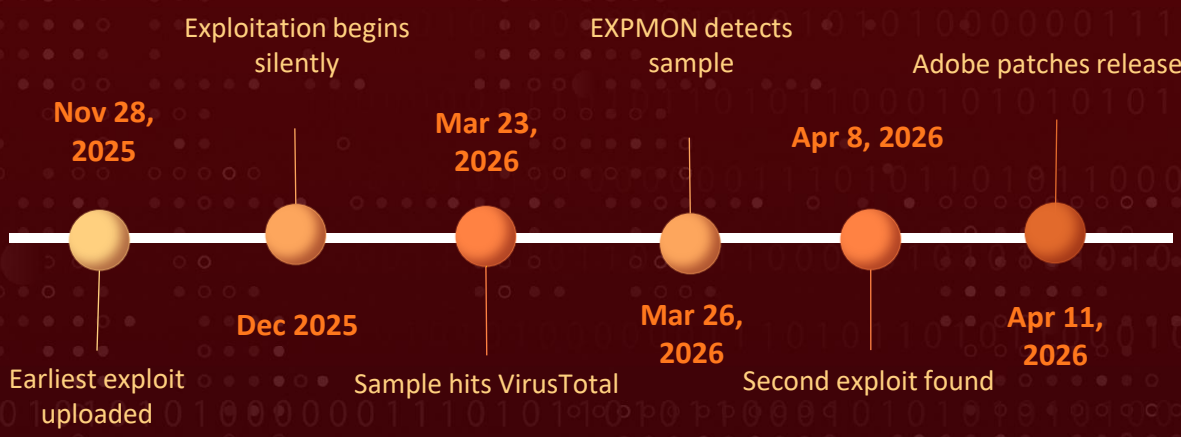
Active Exploitation of Critical Adobe Prototype Pollution Flaw

Date of Publication	Admiralty Code	TA Number
April 13, 2026	A1	TA2026098

Summary

First Seen: December 2025
Affected Products: Adobe Acrobat DC, Adobe Acrobat Reader DC, Adobe Acrobat 2024
Affected Platform: Windows and macOS
Impact: A critical flaw in Adobe Acrobat and Reader, tracked as CVE-2026-34621, is being actively exploited in the wild, turning seemingly harmless PDF files into powerful attack vectors. By abusing a prototype pollution weakness in the application's JavaScript engine, attackers can manipulate core object behavior, gain access to sensitive local files, and quietly exfiltrate data to remote servers, all triggered by simply opening a malicious document. Despite requiring user interaction, the low complexity and lack of authentication make it highly effective in phishing campaigns. Evidence suggests the exploit may have been circulating as a zero-day since late 2025, operating stealthily with low detection rates while enabling attackers to profile victims and potentially escalate to full system compromise.

Timeline



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-34621	Adobe Acrobat and Reader Prototype Pollution Vulnerability	Adobe Acrobat DC, Adobe Acrobat Reader DC, Adobe Acrobat 2024	✓	✓	✓

Vulnerability Details

#1

CVE-2026-34621 is a critical prototype pollution vulnerability affecting Adobe Acrobat and Reader on Windows and macOS. Categorized under CWE-1321, the issue stems from improper handling of object prototype attributes within the application's JavaScript engine. In JavaScript, objects inherit properties from shared prototypes, such as Object.prototype. When user-controlled input is not adequately validated, attackers can tamper with these prototypes, effectively altering how objects behave across the application. This opens the door to serious consequences, including control-flow manipulation and the potential for arbitrary code execution.

#2

At its core, the vulnerability arises from insufficient input sanitization in the embedded JavaScript processing engine used by Acrobat and Reader. By delivering a specially crafted PDF, an attacker can exploit this flaw to interact with privileged internal APIs. The attack chain leverages functions such as util.readFileIntoStream() to access and read files from the local system, enabling the collection of sensitive information. This data is then exfiltrated using the RSS.addFeed() function to an attacker-controlled server, which can respond with additional malicious JavaScript, effectively extending the compromise.

#3

The flaw affects multiple product lines, including Acrobat DC and Acrobat Reader DC (Continuous track) up to version 26.001.21367, as well as Acrobat 2024 (Classic track) up to version 24.001.30356. Both Windows and macOS users are at risk. While exploitation requires the victim to open a malicious PDF file, the overall attack complexity remains low and does not require authentication. This makes the vulnerability particularly dangerous in phishing and social engineering campaigns, where user interaction can be easily coerced.

#4

Initially, Adobe assigned the vulnerability a CVSS v3.1 score of 9.6, reflecting a network-based attack vector. However, on April 12, 2026, the advisory was revised, changing the attack vector from Network to Local, which lowered the score to 8.6. Despite this adjustment, Adobe continues to classify the issue as Critical with a Priority 1 rating, underscoring the urgency for immediate patching.

#5

Notably, the vulnerability has already been observed in active exploitation. Adobe confirmed in-the-wild attacks, and independent researchers, including EXPMON, identified malicious PDF samples exploiting the flaw as early as March 26, 2026. Further analysis suggests that exploitation may have begun as early as December 2025, indicating a significant zero-day exposure window. The exploit appears to function as an initial reconnaissance and data exfiltration mechanism, capable of profiling victims and selectively escalating to more advanced stages such as remote code execution or sandbox escape based on attacker-defined conditions.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-34621	Adobe Acrobat DC (26.001.21367 and earlier), Adobe Acrobat Reader DC (26.001.21367 and earlier), Adobe Acrobat 2024 (24.001.30356 and earlier)	cpe:2.3:a:adobe:acrobat_dc:*:*:*:*:continuous:*:*:* cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:*:continuous:*:*:* cpe:2.3:a:adobe:acrobat:*:*:*:*:classic_2024:*:*:*	CWE-1321

Recommendations

Apply the Emergency Security Update Immediately: Install the latest patched versions released by Adobe without delay. For Acrobat DC and Acrobat Reader DC on the Continuous track, update to version 26.001.21411. For Acrobat 2024 on the Classic 2024 track, update to version 24.001.30362 (Windows) or 24.001.30360 (macOS). Given the confirmed active exploitation, this patch should be prioritized above routine update cycles. End users can update via Help > Check for Updates, and IT administrators should deploy updates through centralized tools such as AIP-GPO, SCUP/SCCM, Apple Remote Desktop, or SSH.

Block and Quarantine Suspicious PDF Files: Implement email gateway and web proxy rules to scrutinize inbound PDF attachments more aggressively. Configure security solutions to sandbox PDF files before delivery to end users. Organizations should consider temporarily restricting the automatic opening of PDF files from untrusted sources until the patching cycle is complete across the environment.

Disable JavaScript in Adobe Reader and Acrobat: As an interim mitigation for systems that cannot be immediately patched, disable JavaScript execution within Adobe Acrobat and Reader by navigating to Edit > Preferences > JavaScript and unchecking the "Enable Acrobat JavaScript" option. This significantly reduces the attack surface for this specific exploit chain, which relies on JavaScript execution within the PDF rendering engine.

Educate Users on PDF-Based Threats: Reinforce end-user security awareness regarding the risks of opening PDF files from unknown or untrusted senders. Remind users that PDF documents can contain active content, including JavaScript, that executes upon opening. Encourage employees to report any suspicious PDF files received via email, messaging platforms, or file-sharing services to the security operations team for analysis.

Vulnerability Management: Maintain an up-to-date inventory of all Adobe Acrobat and Reader installations across the organization, including version numbers and deployment tracks (Continuous vs. Classic). Integrate CVE-2026-34621 into your vulnerability management workflow with the highest priority rating. Continuously monitor for any future updates to this advisory, including potential addition to the CISA Known Exploited Vulnerabilities (KEV) catalog, which would impose binding remediation deadlines for federal agencies and serve as an additional signal to prioritize patching for all organizations.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Discovery	T1083: File and Directory Discovery	
Collection	T1005: Data from Local System	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4:Port	169[.]40[.]2[.]68[:]45191, 188[.]214[.]34[.]20[:]34123
SHA256	65dca34b04416f9a113f09718cbe51e11fd58e7287b7863e37f393ed4d25dde7, 54077a5b15638e354fa02318623775b7a1cc0e8c21e59bcbab333035369e377f

Patch Link

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

References

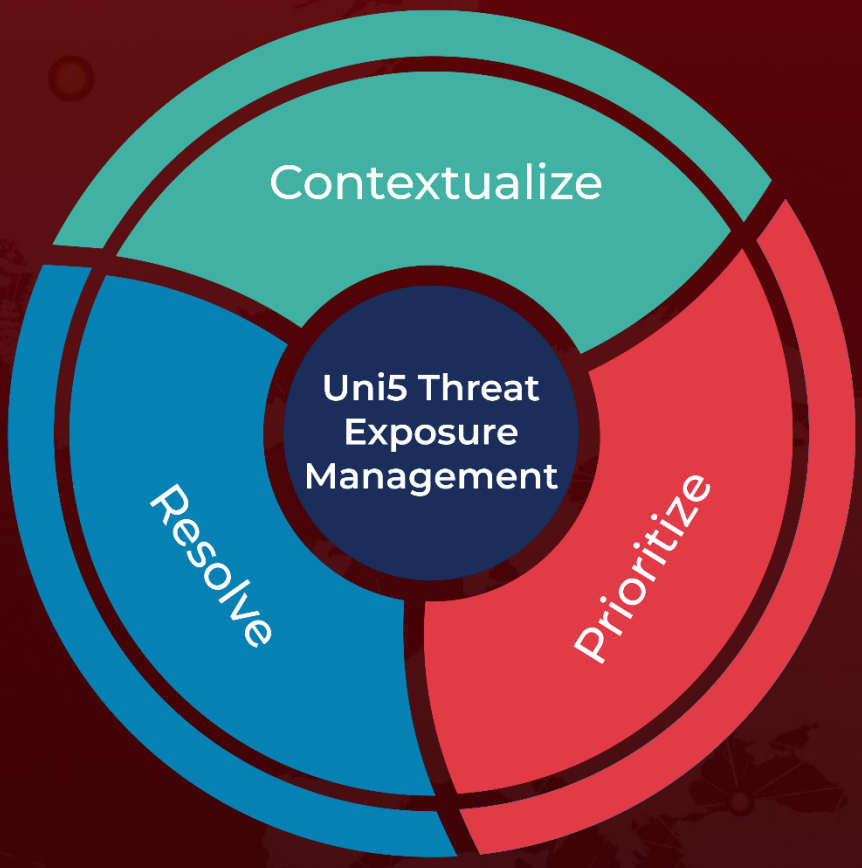
https://helpx.adobe.com/security/products/acrobat/apsb26-43.html

https://justhaifei1.blogspot.com/2026/04/expmon-detected-sophisticated-zero-day-adobe-reader.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 13, 2026 • 9:00 AM

More at www.hivepro.com