Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Adobe Addresses Critical Vulnerabilities Leading to Remote Code Execution

Date of Publication	Admiralty Code	TA Number
September 12, 2024	A1	TA2024353

Summary

First Seen: June 2024
Affected Products: Adobe Acrobat, Adobe Reader
Affected Platforms: Windows and macOS
Impact: Adobe has addressed two critical vulnerabilities in Adobe Acrobat and Reader for both Windows and macOS. The first, CVE-2024-41869, is a use-after-free flaw that can lead to remote code execution. This zero-day vulnerability is urgent, as an active proof-of-concept exploit is circulating. The second vulnerability, CVE-2024-45112, also poses a risk of remote code execution due to a type confusion error. Users should update their software immediately to protect against these serious threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-41869	Adobe Acrobat and Reader Use After Free Vulnerability	Adobe Acrobat and Reader	✓	✗	✓
CVE-2024-45112	Adobe Acrobat and Reader Type Confusion Vulnerability	Adobe Acrobat and Reader	✗	✗	✓

Vulnerability Details

#1

Adobe has addressed two critical vulnerabilities in Acrobat and Reader for Windows and macOS. CVE-2024-41869 is a critical flaw that can let attackers run malicious code remotely, and CVE-2024-45112 involves a type confusion error that also allows remote code execution. Users are at risk of code execution attacks if they don’t update their software.

#2

CVE-2024-41869 is a critical use-after-free (UAF) vulnerability that attackers can exploit to run malicious code. A proof-of-concept (PoC) exploit for this vulnerability has already been identified in the wild, though it doesn't contain a malicious payload at the moment. The PoC exploit triggers crashes, indicating a potential zero-day attack vector. Initially, Adobe attempted to fix the issue with an update in August 2024, but the flaw persisted, leading to the release of an additional, more comprehensive patch in September 2024.

#3

Adobe also patched CVE-2024-45112, a type confusion vulnerability in Acrobat and Reader that can also result in RCE. Attackers can exploit this flaw by delivering a malicious PDF to the victim, potentially gaining full control of the system.

#4

Both vulnerabilities are critical and especially the CVE-2024-41869 is actively being exploited, making it essential for users to apply the latest updates immediately. Users are strongly advised to install the latest security updates from Adobe to protect against these critical vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-41869	Acrobat DC Versions 24.003.20054 and earlier versions (Windows) 24.002.21005 and earlier versions (MacOS), Acrobat Reader DC Versions 24.003.20054 and earlier versions (Windows) 24.002.21005 and earlier versions (MacOS), Acrobat 2024 Versions 24.001.30159 and earlier versions, Acrobat 2020 Versions 20.005.30655 and earlier versions, Acrobat Reader 2020 Versions 20.005.30655 and earlier versions	cpe:2.3:a:adobe:acrobat:*:*:*:*:*:*:*:* cpe:2.3:a:adobe:reader:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-45112		cpe:2.3:a:adobe:acrobat:*:*:*:*:*:*:*:* cpe:2.3:a:adobe:reader:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Update: Ensure you update to the latest versions of Adobe Acrobat Reader and Adobe Acrobat, as critical security flaws CVE-2024-41869 and CVE-2024-45112 have been patched, safeguarding your system against potential exploitation. Users can manually update by selecting Help > Check for Updates within the product.

Remain Vigilant: Refrain from opening PDF files from unknown or suspicious sources until your system is fully updated with the latest security patches to minimize the risk of exploitation.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.005 Exploits	T1588.006 Vulnerabilities	T1566 Phishing	T1059 Command and Scripting Interpreter
T1204 User Execution	T1203 Exploitation for Client Execution		

Patch Details

Users are urged to update to the latest versions of Adobe Acrobat Reader and Adobe Acrobat immediately, as the latest release addresses and patches critical security flaws.

Updated Versions:
Acrobat DC: 24.003.20112
Acrobat Reader DC: 24.003.20112
Acrobat 2024: 24.001.30187
Acrobat 2020: 20.005.30680
Acrobat Reader 2020: 20.005.30680

Link:
https://helpx.adobe.com/security/products/acrobat/apsb24-70.html

References

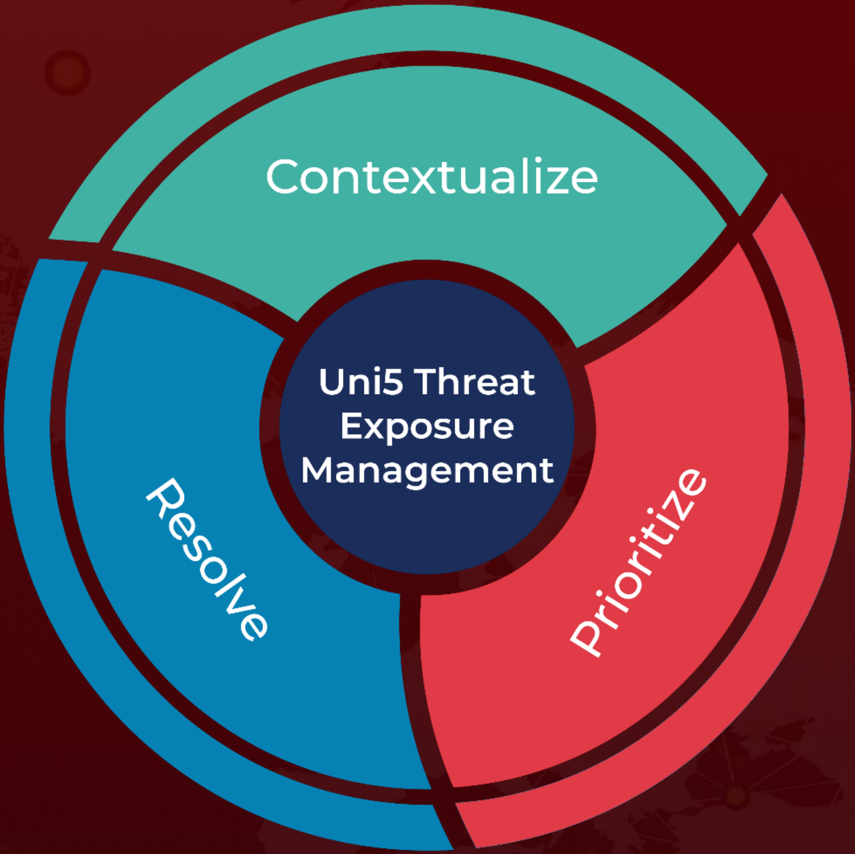
https://helpx.adobe.com/security/products/acrobat/apsb24-70.html

https://x.com/EXPMON_/status/1804642692594569452

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

September 12, 2024 • 6:45 AM

More at www.hivepro.com