certin
Enhancing Cyber Security in India
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2025-0026

Multiple Vulnerabilities in Adobe Products

Original Issue Date: July 15, 2025

Severity Rating: Critical

Software Affected

- Adobe After Effects versions prior to 24.6.7 for Windows and MacOS
- Adobe After Effects versions prior to 25.3 for Windows and MacOS
- Adobe Substance 3D Viewer versions prior to 0.25
- Adobe Audition 24 versions prior to 24.6.7 for Windows and MacOS
- Adobe Audition 25 versions prior to 25.3 for Windows and MacOS
- Adobe InCopy 20 versions prior to 20.4 for Windows and MacOS
- Adobe InCopy 19 versions prior to 19.5.4 for Windows and MacOS
- Adobe InDesign ID20 versions prior to ID20.4 for Windows and MacOS
- Adobe InDesign ID19 versions prior to ID19.5.4 for Windows and MacOS
- Adobe Connect Windows App versions prior to 25.1 for Windows
- Adobe Dimension versions prior to 4.1.3 for Windows and MacOS
- Adobe Substance 3D Stager versions prior to 3.1.3 for Windows and MacOS
- Adobe Illustrator 2025 versions prior to 29.6 for Windows and MacOS
- Adobe Illustrator 2024 versions prior to 28.7.8 for Windows and MacOS
- Adobe FrameMaker 2020 versions prior to Update 9 for Windows
- Adobe FrameMaker 2022 versions prior to Update 7 for Windows
- Adobe Experience Manager (AEM) Forms on JEE versions prior to 6.5.0.0.20250527.0
- Adobe Experience Manager (AEM) Screens 6.5.22 versions prior to FP11.6
- Adobe ColdFusion 2025 versions prior to Update 3
- Adobe ColdFusion 2023 versions prior to Update 15
- Adobe ColdFusion 2021 versions prior to Update 21

Overview

Multiple Vulnerabilities have been reported in Adobe products which could be exploited by an attacker to bypass security restrictions, execute arbitrary code, gain elevated privileges, gain access to sensitive Information, or can cause a denial-of-service condition on the target system.

Target Audience:
System administrators, security teams or end-users of Adobe creative software products.

Risk Assessment:
High risk unauthorized access to sensitive data and system instability.

Impact Assessment:
Potential for data theft, remote code execution and system crash.

Description

Multiple vulnerabilities exist in Adobe products due to memory corruption, incorrect authorization, and other issues.

Successful exploitation of these vulnerabilities could allow an attacker to bypass security restrictions, execute arbitrary code, gain elevated privileges, gain access to sensitive information, or can cause a denial-of-service condition on the target system.

Solution

Apply appropriate updates as mentioned as mentioned in the Adobe Security Bulletin:
https://helpx.adobe.com/security/products/after_effects/apsb25-49.html
https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-54.html
https://helpx.adobe.com/security/products/audition/apsb25-56.html
https://helpx.adobe.com/security/products/incopy/apsb25-59.html
https://helpx.adobe.com/security/products/indesign/apsb25-60.html
https://helpx.adobe.com/security/products/connect/apsb25-61.html
http://helpx.adobe.com/security/products/dimension/apsb25-63.html
https://helpx.adobe.com/security/products/substance3d_stager/apsb25-64.html
https://helpx.adobe.com/security/products/illustrator/apsb25-65.html
https://helpx.adobe.com/security/products/framemaker/apsb25-66.html
https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html
https://helpx.adobe.com/security/products/aem-screens/apsb25-68.html
https://helpx.adobe.com/security/products/coldfusion/apsb25-69.html

Vendor Information

Adobe
https://helpx.adobe.com/security.html

References

Adobe
https://helpx.adobe.com/security/products/after_effects/apsb25-49.html
https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-54.html
https://helpx.adobe.com/security/products/audition/apsb25-56.html
https://helpx.adobe.com/security/products/incopy/apsb25-59.html
https://helpx.adobe.com/security/products/indesign/apsb25-60.html
https://helpx.adobe.com/security/products/connect/apsb25-61.html
http://helpx.adobe.com/security/products/dimension/apsb25-63.html
https://helpx.adobe.com/security/products/substance3d_stager/apsb25-64.html
https://helpx.adobe.com/security/products/illustrator/apsb25-65.html
https://helpx.adobe.com/security/products/framemaker/apsb25-66.html
https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html
https://helpx.adobe.com/security/products/aem-screens/apsb25-68.html
https://helpx.adobe.com/security/products/coldfusion/apsb25-69.html

CVE Name
CVE-2025-47109
CVE-2025-43587
CVE-2025-43582
CVE-2025-43583

CVE-2025-43584
CVE-2025-43580
CVE-2025-47097
CVE-2025-47098
CVE-2025-47099
CVE-2025-47136
CVE-2025-43591
CVE-2025-43592
CVE-2025-43594
CVE-2025-47103
CVE-2025-47134
CVE-2025-27203
CVE-2025-30312
CVE-2025-47135
CVE-2025-27165
CVE-2025-49526
CVE-2025-49527
CVE-2025-49528
CVE-2025-49529
CVE-2025-49530
CVE-2025-49531
CVE-2025-49532
CVE-2025-30313
CVE-2025-49524
CVE-2025-49525
CVE-2025-47121
CVE-2025-47122
CVE-2025-47123
CVE-2025-47124
CVE-2025-47125
CVE-2025-47126
CVE-2025-47127
CVE-2025-47128
CVE-2025-47129
CVE-2025-47130
CVE-2025-47131
CVE-2025-47132
CVE-2025-47133
CVE-2025-47120
CVE-2025-47119
CVE-2025-49533
CVE-2025-49534
CVE-2025-49547
CVE-2025-49535
CVE-2025-49551
CVE-2025-49536
CVE-2025-49537
CVE-2025-49538
CVE-2025-49539
CVE-2025-49540
CVE-2025-49541
CVE-2025-49542
CVE-2025-49543
CVE-2025-49544
CVE-2025-49545

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-22902657

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India