*CYBER ADVISORY*

TLP:CLEAR
15 May 2024

# Multiple Adobe Vulnerabilities

Adobe | Code Execution | Adobe PSIRT | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical vulnerabilities affecting Adobe software.[1] Exploitation of the most critical of the vulnerabilities could allow an attacker to conduct arbitrary cade execution.[2,3]

| Affected Adobe Product | Associated CVE(s) |
|---|---|
| Adobe Acrobat and Reader | CVE-2024-30284, CVE-2024-30310, CVE-2024-34094, CVE-2024-34095, CVE-2024-34096, CVE-2024-34097, CVE-2024-34098, CVE-2024-34099, CVE-2024-34100, CVE-2024-30311, CVE-2024-30312, CVE-2024-34101 |
| Adobe Illustrator | CVE-2024-20791, CVE-2024-20792, CVE-2024-20793 |
| Substance 3D Painter | CVE-2024-30274, CVE-2024-30307, CVE-2024-30308, CVE-2024-30309 |
| Adobe Aero | CVE-2024-30275 |
| Substance 3D Designer | CVE-2024-30281 |
| Adobe Animate | CVE-2024-30282, CVE-2024-30293, CVE-2024-30294, CVE-2024-30298, CVE-2024-30295, CVE-2024-30296, CVE-2024-30297 |
| Adobe FrameMaker | CVE-2024-30283, CVE-2024-30286, CVE-2024-30287, CVE-2024-30288, CVE-2024-30289, CVE-2024-30290, CVE-2024-30291, CVE-2024-30292 |
| Adobe Dreamweaver | CVE-2024-30314 |

**Table 1: Vulnerable Adobe Products**

The Cal-CSIC recommends to immediately apply the appropriate update for the affected Adobe product.

For further information on the affected software and applying updates, please refer to Adobe Product Security Incident Response Team.

## Organization, Source, Reference, and Dissemination Information

| | |
|---|---|
| **Organization Description** | California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state. |
| **Customer Feedback** | If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov. |
| **Source Summary Statement** | This report was compiled from a variety of sources, predominately open-source reporting. |
| **Handling Caveats** | **Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |
| **Information Needs** | *HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5* |

[1] CISA; "Adobe Releases Security Updates for Multiple Products;" https://www.cisa.gov/news-events/alerts/2024/05/15/adobe-releases-security-updates-multiple-products; accessed 15 May 2024

[2] Security Week; "Adobe Patches Critical Flaws in Reader, Acrobat;" https://www.securityweek.com/adobe-patches-critical-flaws-in-reader-acrobat/; accessed 15 May 2024

[3] Qualys; "Microsoft and Adobe Patch Tuesday, May 2024 Security Update Review;" https://blog.qualys.com/vulnerabilities-threat-research/2024/05/14/microsoft-patch-tuesday-may-2024-security-update-review; accessed 15 May 2024