Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0368

Kwetsbaarheden verholpen in Adobe producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-09-2024

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Er zijn kwetsbaarheden verholpen in Adobe producten.

Duiding

De kwetsbaarheden stellen een kwaadwillende in staat aanvallen uit te voeren die leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens

Oplossingen

Adobe heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://helpx.adobe.com/security/products/acrobat/apsb24-70.html
- https://helpx.adobe.com/security/products/after_effects/apsb24-55.html
- https://helpx.adobe.com/security/products/illustrator/apsb24-66.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html
- https://helpx.adobe.com/security/products/photoshop/apsb24-72.html
- https://helpx.adobe.com/security/products/coldfusion/apsb24-71.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-34121	7.8 HIGH
CVE-2024-39381	7.8 HIGH
CVE-2024-39384	7.8 HIGH
CVE-2024-41857	7.8 HIGH
CVE-2024-41859	7.8 HIGH

CVE-2024-41869	7.8 HIGH
CVE-2024-43756	7.8 HIGH
CVE-2024-43758	7.8 HIGH
CVE-2024-43760	7.8 HIGH
CVE-2024-45108	7.8 HIGH
CVE-2024-45109	7.8 HIGH
CVE-2024-45112	8.6 HIGH
CVE-2024-39380	7.8 HIGH
CVE-2024-39382	
CVE-2024-39385	
CVE-2024-41856	7.8 HIGH
CVE-2024-41867	5.5 MEDIUM
CVE-2024-43759	3.3 LOW
CVE-2024-45110	5.5 MEDIUM
CVE-2024-45111	5.5 MEDIUM
CVE-2024-41874	9.8 CRITICAL
CVE-2024-39377	7.8 HIGH
CVE-2024-39378	7.8 HIGH
CVE-2024-41868	5.5 MEDIUM
CVE-2024-41870	5.5 MEDIUM
CVE-2024-41871	5.5 MEDIUM
CVE-2024-41872	5.5 MEDIUM
CVE-2024-41873	5.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-416	Use After Free
CWE-190	Integer Overflow or Wraparound
CWE-787	Out-of-bounds Write
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-20	Improper Input Validation
CWE-121	Stack-based Buffer Overflow
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data

Getroffen producten

adobe
acrobat_2020
acrobat_2024
acrobat_dc
acrobat_reader_2020
acrobat_reader_dc
adobe_after_effects
adobe_premiere_pro
after_effects
illustrator

illustrator_2023
illustrator_2024
photoshop
photoshop_2023
photoshop_2024
premiere_pro
coldfusion_2021
coldfusion_2023
adobe_audition
audition
adobe_media_encoder

Disclaimer