Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0194

Kwetsbaarheden verholpen in Adobe InDesign Desktop

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-06-2026

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

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe InDesign Desktop versies 21.3, 20.5.3 en eerdere versies.

Duiding

De kwetsbaarheden bevinden zich in de wijze waarop Adobe InDesign Desktop malafide bestanden verwerkt. Er zijn stack-based en heap-based buffer overflow kwetsbaarheden die leiden tot geheugenbeschadiging, waardoor een aanvaller code kan uitvoeren met de rechten van de gebruiker die de applicatie draait. Daarnaast is er een Use After Free kwetsbaarheid die eveneens kan leiden tot het uitvoeren van willekeurige code. Verder zijn er out-of-bounds write en read kwetsbaarheden die geheugenbeschadiging veroorzaken en mogelijk leiden tot het uitlekken van gevoelige informatie. Ook is er een NULL Pointer Dereference kwetsbaarheid die een crash van de applicatie veroorzaakt, wat resulteert in een denial-of-service situatie. Al deze kwetsbaarheden worden geactiveerd door het openen van speciaal vervaardigde kwaadaardige bestanden binnen de applicatie. De problemen zijn aanwezig in meerdere versies van Adobe InDesign Desktop.

Oplossingen

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

Referenties

- https://helpx.adobe.com//security/products/indesign/apsb26-58.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-34695	7.8 HIGH
CVE-2026-34696	7.8 HIGH
CVE-2026-34697	7.8 HIGH
CVE-2026-34698	7.8 HIGH
CVE-2026-34699	7.8 HIGH

CVE-2026-34700	7.8 HIGH
CVE-2026-34702	7.8 HIGH
CVE-2026-48293	7.8 HIGH
CVE-2026-34703	5.5 MEDIUM
CVE-2026-34704	5.5 MEDIUM
CVE-2026-34705	5.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-787	Out-of-bounds Write

Getroffen producten

Adobe
InDesign
InDesign Desktop

Disclaimer