



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

Getroffen producten

Adobe
InDesign
InDesign Desktop

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.