



NCSC-2026-0111

Kwetsbaarheid verholpen in Adobe Acrobat

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 13-04-2026

Revisie: 1.0.1

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

Update Revisie 1

New revision

Feiten

Adobe heeft een kwetsbaarheid verholpen in Adobe Acrobat DC, Actobat Reader DC en Acrobat 2024.

Duiding

Een kwaadwillende kan de kwetsbaarheid misbruiken om willekeurige code uit te voeren op het systeem van het slachtoffer. Hiertoe dient de kwaadwillende het slachtoffer ertoe te bewegen een malafide PDF-bestand te openen.

Een malafide PDF-bestand dat op VirusTotal is geüpload, duidt erop dat de kwetsbaarheid sinds ten minste november 2025 wordt misbruikt.

UPDATE Er is publieke exploit code beschikbaar, hiermee is het zeer waarschijnlijk dat er grootschallig misbruik zal plaatsvinden op korte termijn.

Oplossingen

Adobe heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Het NCSC adviseert om deze beveiligingsupdates zo snel mogelijk te installeren. Zie de bijgevoegde referenties voor meer informatie.

Referenties

- <https://helpx.adobe.com/security/products/acrobat/apsb26-43.html>
- <https://justhaifei1.blogspot.com/2026/04/expmon-detected-sophisticated-zero-day-adobe-reader.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-34621	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Getroffen producten

Adobe
Acrobat 2024
Acrobat DC
Acrobat Reader
Acrobat Reader DC

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.