Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0482

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Adobe Photoshop Desktop

Publicatiedatum: 11-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe Photoshop Desktop.

Duiding

De kwetsbaarheden in Adobe Photoshop Desktop omvatten onder andere NULL Pointer Dereference, heap-based buffer overflow, uncontrolled recursion, Divide By Zero, out-of-bounds read en write, en Use After Free. Deze kwetsbaarheden kunnen worden misbruikt door het verwerken van speciaal vervaardigde bestanden.

Afhankelijk van het type kwetsbaarheid kan exploitatie leiden tot het crashen van de applicatie (denial of service), het uitvoeren van willekeurige code met de rechten van de aangemelde gebruiker of het uitlekken van gevoelige informatie door het lezen van geheugen buiten de bedoelde grenzen.

Voor het misbruiken van deze kwetsbaarheden is gebruikersinteractie vereist. Een aanvaller moet hiervoor een gebruiker ertoe bewegen een kwaadaardig bestand te openen. Succesvolle exploitatie kan leiden tot ongeautoriseerde code-uitvoering binnen de context van de betreffende gebruiker of tot het tijdelijk onbeschikbaar worden van de applicatie.

Oplossingen

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

Referenties

- https://www.adobe.com/trust/security/products/photoshop/apsb26-181.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-113569	5.5 MEDIUM
CVE-2026-113571	5.5 MEDIUM
CVE-2026-113575	7.8 HIGH
CVE-2026-113578	5.5 MEDIUM
CVE-2026-114373	5.5 MEDIUM
CVE-2026-115345	5.5 MEDIUM
CVE-2026-116003	7.8 HIGH
CVE-2026-116480	7.8 HIGH
CVE-2026-117546	7.8 HIGH
CVE-2026-117547	7.8 HIGH
CVE-2026-118198	5.5 MEDIUM
CVE-2026-118199	5.5 MEDIUM
CVE-2026-118200	5.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-369	Divide By Zero
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-674	Uncontrolled Recursion
CWE-787	Out-of-bounds Write

Getroffen producten

Adobe
Photoshop

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.