



NCSC-2026-0193

Kwetsbaarheden verholpen in Adobe Dreamweaver 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 Dreamweaver Desktop versies 21.7 en eerder.

Duiding

De kwetsbaarheden kunnen worden misbruikt door een gebruiker een speciaal vervaardigd kwaadaardig bestand te laten openen binnen de applicatie. De kwetsbaarheden omvatten onder andere het uitvoeren van arbitrary code door het openen van kwaadaardige bestanden, het lezen van willekeurige bestanden op het systeem door onvoldoende toegangscontrole en onjuiste autorisatie, het schrijven van bestanden door onjuiste inputvalidatie, en het gebruik van onjuist geïnitieerde pointers wat kan leiden tot geheugenbeschadiging. Exploitatie vereist interactie van de gebruiker met een kwaadaardig bestand en kan leiden tot het uitlekken van gevoelige data, het uitvoeren van code onder de context van de gebruiker, en het manipuleren van bestanden op het systeem.

Oplossingen

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

Referenties

➤ <https://helpx.adobe.com//security/products/dreamweaver/apsb26-62.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-47906	8.6 HIGH
➤ CVE-2026-47907	8.6 HIGH
➤ CVE-2026-47908	7.8 HIGH
➤ CVE-2026-47909	6.3 MEDIUM
➤ CVE-2026-21272	8.6 HIGH
➤ CVE-2026-47910	6.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-284	Improper Access Control
> CWE-824	Access of Uninitialized Pointer
> CWE-863	Incorrect Authorization
> CWE-1395	Dependency on Vulnerable Third-Party Component

Getroffen producten

Adobe
Dreamweaver
Dreamweaver 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.