Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0401

Kwetsbaarheden verholpen in Foxit PDF Reader

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-12-2025

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

Foxit heeft kwetsbaarheden verholpen in Foxit PDF Reader (Specifiek voor versies vóór 2025.2.1, 14.0.1 en 13.2.1 op Windows en MacOS).

Duiding

De kwetsbaarheden omvatten een lokale privilege-escalatie, een use-after-free kwetsbaarheid en een geheugenbeschadiging gerelateerd aan onvoldoende grenzencontrole bij de verwerking van 3D-annotaties. Aanvallers kunnen deze kwetsbaarheden misbruiken om willekeurige code uit te voeren op de getroffen systemen, wat kan leiden tot ongeautoriseerde toegang en systeeminstabiliteit. De use-after-free kwetsbaarheid kan zelfs worden geactiveerd zonder gebruikersinteractie, wat het risico vergroot, vooral in omgevingen waar PDF-bestanden vaak worden geopend.

Oplossingen

Foxit heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.foxit.com/support/security-bulletins.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-13941	8.5 HIGH
CVE-2025-57779	
CVE-2025-58085	
CVE-2025-59488	
CVE-2025-66493	5.3 MEDIUM
CVE-2025-66494	5.3 MEDIUM
CVE-2025-66495	5.3 MEDIUM

CVE-2025-66496	**5.3 MEDIUM**
CVE-2025-66497	**5.3 MEDIUM**
CVE-2025-66498	**5.3 MEDIUM**
CVE-2025-66499	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-416	Use After Free
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-787	Out-of-bounds Write

Getroffen producten

Foxit
PDF Editor
PDF Reader

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.