



NCSC-2024-0500

Kwetsbaarheden verholpen in Foxit PDF Reader en PDF Editor

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 31-12-2024

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.

Duiding

De kwetsbaarheden omvatten een remote code execution kwetsbaarheid door onjuiste validatie van door de gebruiker aangeleverde data in AcroForms, een geheugenbeschadiging gerelateerd aan AcroForm-functionaliteit, en een lokale privilege-escalatie kwetsbaarheid die kan worden misbruikt via de productinstallateur. Daarnaast zijn er use-after-free kwetsbaarheden die kunnen worden geëxploiteerd via speciaal gemaakte PDF-documenten of kwaadaardige websites. Deze kwetsbaarheden vereisen gebruikersinteractie en kunnen leiden tot de uitvoering van willekeurige code op het systeem.

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-2024-12751	7.8 HIGH
➤ CVE-2024-12752	7.8 HIGH
➤ CVE-2024-12753	6.7 MEDIUM
➤ CVE-2024-47810	8.8 HIGH
➤ CVE-2024-49576	8.8 HIGH

CWE's

CWE	Beschrijving
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-125	Out-of-bounds Read
> CWE-416	Use After Free

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.