



NCSC-2024-0483

Kwetsbaarheden verholpen in Adobe Connect

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-12-2024

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

Adobe heeft kwetsbaarheden verholpen in Adobe Connect (Versies 12.6, 11.4.7 en eerder).

Duiding

De kwetsbaarheden omvatten zowel opgeslagen als gereflecteerde Cross-Site Scripting (XSS) die aanvallers in staat stellen om kwaadaardige scripts in te voegen en uit te voeren in de browsers van gebruikers. Dit kan leiden tot ongeautoriseerde acties in de context van de sessie van het slachtoffer, wat gevolgen kan hebben voor de integriteit en vertrouwelijkheid van gebruikersdata. Daarnaast is er een kwetsbaarheid voor onjuiste toegangscontrole die aanvallers in staat stelt om beveiligingsmaatregelen te omzeilen, wat kan leiden tot ongeautoriseerde toegang tot gevoelige informatie zonder enige gebruikersinteractie.

Oplossingen

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

Referenties

➤ <https://helpx.adobe.com/security/products/connect/apsb24-99.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-54032	9.3 CRITICAL
➤ CVE-2024-54034	8.0 HIGH
➤ CVE-2024-54035	7.3 HIGH
➤ CVE-2024-54036	8.2 HIGH
➤ CVE-2024-54037	7.3 HIGH
➤ CVE-2024-54039	5.4 MEDIUM
➤ CVE-2024-49550	6.1 MEDIUM
➤ CVE-2024-54040	5.4 MEDIUM

> CVE-2024-54041	5.4 MEDIUM
> CVE-2024-54042	5.4 MEDIUM
> CVE-2024-54043	5.4 MEDIUM
> CVE-2024-54044	5.4 MEDIUM
> CVE-2024-54045	5.4 MEDIUM
> CVE-2024-54046	5.4 MEDIUM
> CVE-2024-54047	5.4 MEDIUM
> CVE-2024-54048	5.4 MEDIUM
> CVE-2024-54049	6.1 MEDIUM
> CVE-2024-54050	3.1 LOW
> CVE-2024-54051	3.1 LOW
> CVE-2024-54038	4.3 MEDIUM

CWE's

CWE	Beschrijving
> CVE-601	URL Redirection to Untrusted Site ('Open Redirect')
> CVE-285	Improper Authorization
> CVE-284	Improper Access Control
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

adobe
adobe_connect

connect

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.