



# NCSC-2024-0273

## Kwetsbaarheden ontdekt in Kiloview P1 4G Video Encoder en P2 4G Video Encoder

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 02-07-2024

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Er zijn kwetsbaarheden ontdekt in Kiloview P1 en P2.

Kiloview P1 en P2 zijn hardware-oplossingen om beeldinformatie in HDMI-formaat te kunnen streamen. De firmware van deze systemen bevat een aantal ernstige kwetsbaarheden, waardoor een kwaadwillende aanvallen kan uitvoeren die kunnen leiden tot de volgende categorieën schade: • Cross-Site-Scripting (XSS) • Omzeilen van authenticatie • Denial-of-Service (DoS) • Manipulatie van gegevens • (Remote) code execution (Administrator/Root rechten) • Toegang tot gevoelige gegevens

## Duiding

De firmware maakt gebruik van een aantal hard-coded credentials, waardoor een kwaadwillende toegang kan krijgen tot het systeem.

Ook is het mogelijk om zonder authenticatie de firmware te vervangen, waardoor de werking van het systeem kan worden gemanipuleerd.

Er is geen encryptie op de configuratie webinterface waardoor een aanvaller de communicatie kan afluisteren en credentials kan onderscheppen.

Elk van de kwetsbaarheden afzonderlijk maakt misbruik mogelijk. In keten echter, is totale overname van het systeem mogelijk, waarmee de kwaadwillende volledige controle heeft over het systeem en de streaming data.

## Oplossingen

De leverancier heeft besloten de kwetsbaarheden niet te verhelpen in de meest recente update van de firmware. Bij navraag door het NCSC geeft de leverancier ook geen indicatie van een oplossingstermijn. Wel heeft de leverancier updates uitgebracht voor de centrale serversystemen om misbruik daar tegen te gaan.

Het NCSC adviseert daarom dan ook om op basis van deze informatie een risico-afweging te maken omtrent de inzet en het gebruik van deze systemen.

## Referenties

➤ <https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273>

## Kwetsbaarheden

CVE	CVSS Score
<a href="#">&gt; CVE-2023-41917</a>	
<a href="#">&gt; CVE-2023-41918</a>	
<a href="#">&gt; CVE-2023-41919</a>	
<a href="#">&gt; CVE-2023-41920</a>	
<a href="#">&gt; CVE-2023-41921</a>	
<a href="#">&gt; CVE-2023-41922</a>	
<a href="#">&gt; CVE-2023-41923</a>	
<a href="#">&gt; CVE-2023-41926</a>	
<a href="#">&gt; CVE-2023-41927</a>	
<a href="#">&gt; CVE-2023-41928</a>	

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-20</a>	Improper Input Validation
<a href="#">&gt; CWE-305</a>	Authentication Bypass by Primary Weakness
<a href="#">&gt; CWE-306</a>	Missing Authentication for Critical Function
<a href="#">&gt; CWE-327</a>	Use of a Broken or Risky Cryptographic Algorithm
<a href="#">&gt; CWE-494</a>	Download of Code Without Integrity Check
<a href="#">&gt; CWE-521</a>	Weak Password Requirements
<a href="#">&gt; CWE-522</a>	Insufficiently Protected Credentials
<a href="#">&gt; CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

[> CWE-798](#)

Use of Hard-coded Credentials

## Getroffen producten

### kiloview

p1

p2

## 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.