Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CVE-2023-41917	
CVE-2023-41918	
CVE-2023-41919	
CVE-2023-41920	
CVE-2023-41921	
CVE-2023-41922	
CVE-2023-41923	
CVE-2023-41926	
CVE-2023-41927	
CVE-2023-41928	

CWE's

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

CWE-798	Use of Hard-coded Credentials

Getroffen producten

kiloview
p1
p2

Disclaimer