Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0001

Kwetsbaarheden verholpen in Hanwha camera systemen

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-01-2026

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

Hanwha heeft kwetsbaarheden verholpen in verschillende camera systemen, waaronder issues met XML-validatie, certificaatvalidatie, permissiebeheer voor gastaccounts, video-analyse en een hardcoded encryptiesleutel.

Duiding

De kwetsbaarheden omvatten onder andere een probleem met de validatie van binnenkomende XML-verzoeken, wat XSS-aanvallen op gebruikers kan faciliteren. Daarnaast is er een tekortkoming in de clientservice van de camera die certificaten niet correct valideert, wat de apparaten blootstelt aan beveiligingsrisico's. Een andere kwetsbaarheid betreft het beheer van gastaccounts in industriële controlesystemen, wat ongeautoriseerde toegang tot gevoelige functionaliteiten kan toestaan. Verder is er een probleem met onjuiste invoervalidatie in camera video-analyse, waardoor aanvallers willekeurige commando's op de pc van een gebruiker kunnen uitvoeren. Tot slot is er een kwetsbaarheid in Device Manager door een hardcoded encryptiesleutel die ongeautoriseerde decryptie van gevoelige informatie mogelijk maakt.

Oplossingen

Hanwha heeft firmware patches uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://www.hanwhavision.com/wp-content/uploads/2025/12/Camera-Vulnerability-ReportCVE-2025-5259852601-8075.pdf

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-8075	5.8 MEDIUM
› CVE-2025-52598	6.3 MEDIUM
› CVE-2025-52599	6.3 MEDIUM
› CVE-2025-52600	8.9 HIGH
› CVE-2025-52601	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-269	Improper Privilege Management
CWE-295	Improper Certificate Validation
CWE-321	Use of Hard-coded Cryptographic Key

Getroffen producten

Hanwha
LNV-6022R Firmware
PNM-7002VD Firmware
PNM-9000VD Firmware
PNM-9002VQ Firmware
PNM-9084QZ Firmware
PNM-9084QZ1 Firmware
PNM-9084RQZ Firmware
PNM-9084RQZ1 Firmware
PNM-9085RQZ Firmware

PNM-9085RQZ1 Firmware
PNM-9322VQP Firmware
QND-6011 Firmware
QND-8010R Firmware
QND-8020R Firmware
QNF-8010 Firmware
QNO-6010R Firmware
QNO-8020R Firmware
QNP-6230H Firmware
QNP-6230RH Firmware
QNP-6250 Firmware
QNP-6250H Firmware
QNP-6250R Firmware
QNP-6320 Firmware
QNP-6320H Firmware
QNP-6320R Firmware

QNV-8080R Firmware
XNB-6002 Firmware
XNB-6003 Firmware
XNB-8002 Firmware
XNB-8003 Firmware
XNB-9002 Firmware
XNB-9003 Firmware
XND-6083RV Firmware
XND-8082RF Firmware
XND-8082RV Firmware
XND-8083RV Firmware
XND-9082RV Firmware
XND-C6083RV Firmware
XND-C7083RV Firmware
XND-C8083RV Firmware
XND-C9083RV Firmware

XNF-9010RVM Firmware
XNF-9013RV Firmware
XNO-6083R Firmware
XNO-6123R Firmware
XNO-8082R Firmware
XNO-8083R Firmware
XNO-9083R Firmware
XNO-C6083R Firmware
XNO-C7083R Firmware
XNO-C8083R Firmware
XNO-C9083R Firmware
XNP-6400R Firmware
XNP-6400RW Firmware
XNP-8250 Firmware
XNP-8250R Firmware
XNP-8300RW Firmware

XNP-9250 Firmware
XNP-9300RW Firmware
XNV-6083R Firmware
XNV-6083RZ Firmware
XNV-6083Z Firmware
XNV-6123R Firmware
XNV-8082R Firmware
XNV-8083R Firmware
XNV-8083RZ Firmware
XNV-8083Z Firmware
XNV-8093R Firmware
XNV-9082R Firmware
XNV-9083R Firmware
XNV-9083RZ Firmware
XNV-C6083R Firmware
XNV-C7083R Firmware

XNV-C8083R Firmware
XNV-C9083R Firmware
pnm-7002vd_firmware
pnm-9000vq_firmware
pnm-9002vq_firmware
pnm-9080vq_firmware
pnm-9081vq_firmware
pnm-9320vqp_firmware
pnm-9321vqp_firmware
qnp-6230_firmware
qnp-6320_firmware
tnb-6030_firmware
xnb-6001_firmware
xnb-6002_firmware
xnb-6005_firmware
xnd-6010_firmware
xnd-6020r_firmware
xnd-6080rv_firmware
xnd-6080v_firmware
xnd-6081f_firmware
xnd-6081rev_firmware
xnd-6081rf_firmware
xnd-6081rv_firmware
xnd-6081v_firmware
xnd-6081vz_firmware

xnd-6083rv_firmware
xnd-8020f_firmware
xnd-8030r_firmware
xnd-8080rv_firmware
xnd-8081fz_firmware
xnd-8081rev_firmware
xnd-8081vz_firmware
xnd-8082rf_firmware
xnd-8082rv_firmware
xnd-9082rf_firmware
xnd-l6080rv_firmware
xnd-l6080v_firmware
xnf-8010r_firmware
xnf-8010rv_firmware
xnf-8010rw_firmware
xnf-9010rs_firmware
xnf-9010rv_firmware
xnf-9010rvm_firmware
xno-6020r_firmware
xno-6080r_firmware
xno-6085r_firmware
xno-6120r_firmware
xno-8030r_firmware
xno-8040r_firmware
xno-8080r_firmware

xno-l6080r_firmware
xnp-6040h_firmware
xnp-6120h_firmware
xnp-6320_firmware
xnp-6320h_firmware
xnp-6320hs_firmware
xnp-6320rh_firmware
xnp-6321_firmware
xnp-6321h_firmware
xnp-6400_firmware
xnp-6550rh_firmware
xnp-9250r_firmware
xnv-6010_firmware
xnv-6011_firmware
xnv-6011w_firmware
xnv-6012_firmware
xnv-6012m_firmware
xnv-6020r_firmware
xnv-6022rm_firmware
xnv-6080_firmware
xnv-6080r_firmware
xnv-6080rs_firmware
xnv-6080rsa_firmware
xnv-6081_firmware
xnv-6081r_firmware

xnv-6081re_firmware
xnv-6081z_firmware
xnv-6083r_firmware
xnv-6085_firmware
xnv-6120r_firmware
xnv-6120rs_firmware
xnv-6123r_firmware
xnv-8020r_firmware
xnv-8030r_firmware
xnv-8040r_firmware
xnv-8080r_firmware
xnv-8080rsa_firmware
xnv-8081r_firmware
xnv-l6080_firmware
xnv-l6080r_firmware
xnz-6320_firmware
xnz-l6320_firmware
xnz-l6320a_firmware

Disclaimer