NVD DB Update

CVE-2023-34552 - Score: 8.8

Components:

ezviz cs-c6n-b0-1g2wf -
ezviz cs-c6n-b0-1g2wf firmware *

Description:

In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8 mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214.

Main problems:

787 "Out-of-bounds Write"

https://cybersword.tech
www.linkedin.com/in/cybersword-tech
ph1sher
@davidwowa