# CVE Detail – CVE-2020-11624

An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.58449

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-521: Weak Password Requirements

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-16: Dictionary-based Password Attack
* CAPEC-49: Password Brute Forcing
* CAPEC-509: Kerberoasting
* CAPEC-55: Rainbow Table Password Cracking
* CAPEC-555: Remote Services with Stolen Credentials
* CAPEC-561: Windows Admin Shares with Stolen Credentials
* CAPEC-565: Password Spraying
* CAPEC-70: Try Common or Default Usernames and Passwords

## ATT&CK Techniques

* T1110.001: Password Guessing
* T1133: External Remote Services
* T1110.002: Password Cracking
* T1021.002: SMB/Windows Admin Shares
* T1021: Remote Services
* T1078.001: Default Accounts
* T1110.003: Password Spraying
* T1110: Brute Force
* T1114.002: Remote Email Collection
* T1558.003: Kerberoasting

## Used By (Actors/Tools)

* Stuxnet (malware)
* reGeorg (malware)
* Linux Rabbit (malware)
* RansomHub (malware)
* Pony (malware)
* HyperStack (malware)
* Bad Rabbit (malware)
* Emotet (malware)
* Olympic Destroyer (malware)
* Mafalda (malware)
* Hildegard (malware)
* P.A.S. Webshell (malware)
* Regin (malware)
* Conti (malware)
* Diavol (malware)
* Doki (malware)
* Lucifer (malware)
* BlackEnergy (malware)
* zwShell (malware)
* NotPetya (malware)
* Conficker (malware)
* China Chopper (malware)
* Chaos (malware)
* Anchor (malware)
* SeaDuke (malware)
* Duqu (malware)
* Xbash (malware)
* LightNeuron (malware)
* LockBit 3.0 (malware)
* Caterpillar WebShell (malware)
* Royal (malware)
* Shamoon (malware)
* BlackByte Ransomware (malware)
* Ryuk (malware)
* Pysa (malware)
* LockBit 2.0 (malware)
* SpeakUp (malware)
* Cobalt Strike (malware)
* Valak (malware)
* Kivars (malware)
* MacMa (malware)
* Kwampirs (malware)
* Kinsing (malware)
* QakBot (malware)
* Zox (malware)
* Net Crawler (malware)
* HermeticWizard (malware)
* Net (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Brute Ratel C4 (tool)
* MailSniper (tool)
* CrackMapExec (tool)
* Rubeus (tool)
* PsExec (tool)
* Indrik Spider (intrusion-set)
* C0027 (campaign)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Operation CuckooBees (campaign)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* CostaRicto (campaign)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* APT28 (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* HEXANE (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* Storm-1811 (intrusion-set)
* Akira (intrusion-set)
* LAPSUS$ (intrusion-set)
* Chimera (intrusion-set)
* ToddyCat (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* Threat Group-1314 (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* FIN8 (intrusion-set)
* Scattered Spider (intrusion-set)
* Blue Mockingbird (intrusion-set)
* FIN4 (intrusion-set)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* APT28 Nearest Neighbor Campaign (campaign)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Salt Typhoon (intrusion-set)
* APT3 (intrusion-set)
* Operation MidnightEclipse (campaign)
* C0032 (campaign)
* APT1 (intrusion-set)
* HomeLand Justice (campaign)
* FIN5 (intrusion-set)
* APT33 (intrusion-set)
* Cutting Edge (campaign)
* GOLD SOUTHFIELD (intrusion-set)
* Silent Librarian (intrusion-set)
* APT18 (intrusion-set)
* Orangeworm (intrusion-set)
* Deep Panda (intrusion-set)
* Star Blizzard (intrusion-set)

## Affected Products

* cpe:2.3:o:avertx:hd838\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:avertx:hd438\_firmware:-:\*:\*:\*:\*:\*:\*:\*