IP Camera Security Report

Camera IP: 192.168.67.13

Camera Detail:

Vendor: Dahua
Firmware Version: Unknown

Services:

Port: 8556
Service: rtsp
Product: VLC rtspd
Version: 1.1.9

Vulnerabilities Found:

- CVE-2017-7927

A Use of Password Hash Instead of Password for Authentication issue was discovered in Dahua DH-IPC-HDBW23A0RN-ZS, DH-IPC-HDBW13A0SN, DH-IPC-HDW1XXX, DH-IPC-HDW2XXX, DH-IPC-HDW4XXX, DH-IPC-HFW1XXX, DH-IPC-HFW2XXX, DH-IPC-HFW4XXX, DH-SD6CXX, DH-NVR1XXX, DH-HCVR4XXX, DH-HCVR5XXX, DHI-HCVR51A04HE-S3, DHI-HCVR51A08HE-S3, and DHI-HCVR58A32S-S2 devices. The use of password hash instead of password for authentication vulnerability was identified, which could allow a malicious user to bypass authentication without obtaining the actual password.

Mitigation:

1. Update affected devices with security patches from the vendor
2. Change default passwords to strong, unique ones

- CVE-2017-6343

The web interface on Dahua DHI-HCVR7216A-S3 devices with NVR Firmware 3.210.0001.10 2016-06-06, Camera Firmware 2.400.0000.28.R 2016-03-29, and SmartPSS Software 1.16.1 2017-01-19 allows remote attackers to obtain login access by leveraging knowledge of the MD5 Admin Hash without knowledge of the corresponding password, a different vulnerability than CVE-2013-6117.

Mitigation:

1. Update firmware and software to patched versions
2. Implement strong password policies
3. Monitor and restrict access to the web interface

IP Camera Security Report

- CVE-2017-3223

Dahua IP camera products using firmware versions prior to V2.400.0000.14.R.20170713 include a version of the Sonia web interface that may be vulnerable to a stack buffer overflow. Dahua IP camera products include an application known as Sonia (/usr/bin/sonia) that provides the web interface and other services for controlling the IP camera remotely. Versions of Sonia included in firmware versions prior to DH_IPC-Consumer-Zi-Themis_Eng_P_V2.408.0000.11.R.20170621 do not validate input data length for the 'password' field of the web interface. A remote, unauthenticated attacker may submit a crafted POST request to the IP camera's Sonia web interface that may lead to out-of-bounds memory operations and loss of availability or remote code execution. The issue was originally identified by the researcher in firmware version DH_IPC-HX1X2X-Themis_EngSpnFrn_N_V2.400.0000.30.R.20160803.

Mitigation:

Update the firmware to version DH_IPC-ACK-Themis_Eng_P_V2.400.0000.14.R.20170713 to mitigate the vulnerability.

- CVE-2017-9317

Privilege escalation vulnerability found in some Dahua IP devices. Attacker in possession of low privilege account can gain access to credential information of high privilege account and further obtain device information or attack the device.

Mitigation:

1. Update devices to versions released after September 2017
2. Change default credentials and ensure strong passwords
3. Monitor and restrict access to high privilege accounts

- CVE-2013-6117

Dahua DVR 2.608.0000.0 and 2.608.GV00.0 allows remote attackers to bypass authentication and obtain sensitive information including user credentials, change user passwords, clear log files, and perform other actions via a request to TCP port 37777.

Mitigation:

Refer to the vendor and update to the latest patch.

- CVE-2013-3612

Dahua DVR appliances have a hardcoded password for (1) the root account and (2) an unspecified "backdoor" account, which makes it easier for remote attackers to obtain administrative access via authorization requests involving (a) ActiveX, (b) a standalone client, or (c) unknown other vectors.

Mitigation:

Refer to the vendor and update to the latest patch.

IP Camera Security Report

- CVE-2017-6341

Dahua DHI-HCVR7216A-S3 devices with NVR Firmware 3.210.0001.10 2016-06-06, Camera Firmware 2.400.0000.28.R 2016-03-29, and SmartPSS Software 1.16.1 2017-01-19 send cleartext passwords in response to requests from the Web Page, Mobile Application, and Desktop Application interfaces, which allows remote attackers to obtain sensitive information by sniffing the network, a different vulnerability than CVE-2013-6117.

Mitigation:

1. Update firmware to the latest secure versions
2. Change passwords to ensure they are not transmitted in cleartext
3. Monitor network traffic for any suspicious activities

- CVE-2013-5754

The authorization implementation on Dahua DVR appliances accepts a hash string representing the current date for the role of a master password, which makes it easier for remote attackers to obtain administrative access and change the administrator password via requests involving (1) ActiveX, (2) a standalone client, or (3) unspecified other vectors, a different vulnerability than CVE-2013-3612.

Mitigation:

Refer to the vendor and update to the latest patch.

- CVE-2017-6432

An issue was discovered on Dahua DHI-HCVR7216A-S3 3.210.0001.10 build 2016-06-06 devices. The Dahua DVR Protocol, which operates on TCP Port 37777, is an unencrypted, binary protocol. Performing a Man-in-the-Middle attack allows both sniffing and injections of packets, which allows creation of fully privileged new users, in addition to capture of sensitive information.

Mitigation:

1. Disable remote access if not required.
2. Implement strong network segmentation.
3. Monitor network traffic for any suspicious activities.

- CVE-2019-9676

Buffer overflow vulnerability found in some Dahua IP Camera devices IPC-HFW1XXX,IPC-HDW1XXX,IPC-HFW2XXX Build before 2018/11. The vulnerability exits in the function of redirection display for serial port printing information, which can not be used by product basic functions. After an attacker logs in locally, this vulnerability can be exploited to cause device restart or arbitrary code execution. Dahua has identified the corresponding security problems in the static code auditing process, so it has gradually deleted this function, which is no longer available in the newer devices and softwares. Dahua has released versions of the affected products to fix the vulnerability.

Mitigation:

1. Update affected Dahua IP Cameras to the latest firmware versions provided by Dahua.

IP Camera Security Report

- CVE-2017-9314

Authentication vulnerability found in Dahua NVR models NVR50XX, NVR52XX, NVR54XX, NVR58XX with software before DH_NVR5xxx_Eng_P_V2.616.0000.0.R.20171102. Attacker could exploit this vulnerability to gain access to additional operations by means of forging json message.

Mitigation:

1. Update affected systems to the patched version DH_NVR5xxx_Eng_P_V2.616.0000.0.R.20171102 or later.
2. Monitor network traffic for any suspicious activity.
3. Implement strong password policies and multi-factor authentication.

- CVE-2008-0225

Heap-based buffer overflow in the rmff_dump_cont function in input/libreal/rmff.c in xine-lib 1.1.9 and earlier allows remote attackers to execute arbitrary code via the SDP Abstract attribute in an RTSP session, related to the rmff_dump_header function and related to disregarding the max field. NOTE: some of these details are obtained from third party information.

Mitigation:

Refer to the vendor and update to the latest patch.

- CVE-2013-3614

Dahua DVR appliances have a small value for the maximum password length, which makes it easier for remote attackers to obtain access via a brute-force attack.

Mitigation:

Refer to the vendor and update to the latest patch.

- CVE-2019-3948

The Amcrest IP2M-841B V2.520.AC00.18.R, Dahua IPC-XXBXX V2.622.0000000.9.R, Dahua IPC HX5X3X and HX4X3X V2.800.0000008.0.R, Dahua DH-IPC HX883X and DH-IPC-HX863X V2.622.0000000.7.R, Dahua DH-SD4XXXXX V2.623.0000000.7.R, Dahua DH-SD5XXXXX V2.623.0000000.1.R, Dahua DH-SD6XXXXX V2.640.0000000.2.R and V2.623.0000000.1.R, Dahua NVR5XX-4KS2 V3.216.0000006.0.R, Dahua NVR4XXX-4KS2 V3.216.0000006.0.R, and NVR2XXX-4KS2 do not require authentication to access the HTTP endpoint /videotalk. An unauthenticated, remote person can connect to this endpoint and potentionally listen to the audio of the capturing device.

Mitigation:

1. Disable access to the /videotalk endpoint if not essential
2. Implement strong authentication mechanisms
3. Regularly monitor and audit access to sensitive endpoints

IP Camera Security Report

- CVE-2013-3613

Dahua DVR appliances do not properly restrict UPnP requests, which makes it easier for remote attackers to obtain access via vectors involving a replay attack against the TELNET port.

Mitigation:

Refer to the vendor and update to the latest patch.

- CVE-2017-9316

Firmware upgrade authentication bypass vulnerability was found in Dahua IPC-HDW4300S and some IP products. The vulnerability was caused by internal Debug function. This particular function was used for problem analysis and performance tuning during product development phase. It allowed the device to receive only specific data (one direction, no transmit) and therefore it was not involved in any instance of collecting user privacy data or allowing remote code execution.

Mitigation:

1. Apply patches or firmware updates provided by Dahua Technologies.
2. Restrict network access to vulnerable devices.
3. Monitor for unauthorized firmware modifications.

- CVE-2017-9315

Customer of Dahua IP camera or IP PTZ could submit relevant device information to receive a time limited temporary password from Dahua authorized dealer to reset the admin password. The algorithm used in this mechanism is potentially at risk of being compromised and subsequently utilized by attacker.

Mitigation:

1. Update to the latest firmware provided by Dahua Technologies
2. Change default passwords and implement strong, unique passwords
3. Monitor and restrict access to the devices

- CVE-2017-7253

Dahua IP Camera devices 3.200.0001.6 can be exploited via these steps: 1. Use the default low-privilege credentials to list all users via a request to a certain URI. 2. Login to the IP camera with admin credentials so as to obtain full control of the target IP camera. During exploitation, the first JSON object encountered has a "Component error: login challenge!" message. The second JSON object encountered has a result indicating a successful admin login.

Mitigation:

1. Change default credentials immediately to prevent unauthorized access.
2. Regularly monitor and audit access logs for any suspicious activities.

IP Camera Security Report

- CVE-2017-6342

An issue was discovered on Dahua DHI-HCVR7216A-S3 devices with NVR Firmware 3.210.0001.10 2016-06-06, Camera Firmware 2.400.0000.28.R 2016-03-29, and SmartPSS Software 1.16.1 2017-01-19. When SmartPSS Software is launched, while on the login screen, the software in the background automatically logs in as admin. This allows sniffing sensitive information identified in CVE-2017-6341 without prior knowledge of the password. This is a different vulnerability than CVE-2013-6117.

Mitigation:

1. Disable automatic login features on SmartPSS Software.
2. Implement strong password policies for all system accounts.
3. Monitor network traffic for any suspicious activities.

- CVE-2013-3615

Dahua DVR appliances use a password-hash algorithm with a short hash length, which makes it easier for context-dependent attackers to discover cleartext passwords via a brute-force attack.

Mitigation:

Refer to the vendor and update to the latest patch.

- CVE-2017-7925

A Password in Configuration File issue was discovered in Dahua DH-IPC-HDBW23A0RN-ZS, DH-IPC-HDBW13A0SN, DH-IPC-HDW1XXX, DH-IPC-HDW2XXX, DH-IPC-HDW4XXX, DH-IPC-HFW1XXX, DH-IPC-HFW2XXX, DH-IPC-HFW4XXX, DH-SD6CXX, DH-NVR1XXX, DH-HCVR4XXX, DH-HCVR5XXX, DHI-HCVR51A04HE-S3, DHI-HCVR51A08HE-S3, and DHI-HCVR58A32S-S2 devices. The password in configuration file vulnerability was identified, which could lead to a malicious user assuming the identity of a privileged user and gaining access to sensitive information.

Mitigation:

1. Change default passwords on affected devices.
2. Regularly update firmware to patch security vulnerabilities.
3. Implement strong password policies and encryption methods.

- Open RTSP Stream Without Authentication

The Real-Time Streaming Protocol (RTSP) is publicly accessible without login credentials.

Mitigation:

1. Enable authentication for RTSP.
2. If not needed, disable RTSP streaming.
3. Restrict RTSP access to trusted IP addresses only.

IP Camera Security Report

- Weak or No Encryption for Video Streams

The video feed is transmitted without encryption, allowing attackers to intercept footage.

Mitigation:

1. Enable end-to-end encryption for video streams.
2. Use secured VPN tunnels for remote access.
3. If possible, implement AES-256 encryption for streaming.