Security Notice - Statement on security risks exist in some Dahua software products

Notice ID: *DHCC-SN-202212-001*

First Published: *2022-12-20*

Summary

Recently, some security risks are found in some Dahua software products, the more information are described below in more depth.

1.**CVE-2022-45423：**

Some Dahua software products have a vulnerability of unauthenticated request of MQTT credentials. An attacker can obtain encrypted MQTT credentials by sending a specific crafted packet to the vulnerable interface.
Severity：Medium
Base Score：5.3(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

2.**CVE-2022-45424**：

Some Dahua software products have a vulnerability of unauthenticated request of AES crypto key. An attacker can obtain the AES crypto key by sending a specific crafted packet to the vulnerable interface.
Severity：High
Base Score：7.5(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

3.**CVE-2022-45425**：

Some Dahua software products have a vulnerability of using of hard-coded cryptographic key. An attacker can obtain the AES crypto key by exploiting this vulnerability.
Severity：High
Base Score：7.5(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

4.**CVE-2022-45426**：

Some Dahua software products have a vulnerability of unrestricted download of file. After obtaining the permissions of ordinary users, by sending a specific crafted packet to the vulnerable interface, an attacker can download arbitrary files.
Severity：High

Base Score：7.7(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

5.**CVE-2022-45427**：

Some Dahua software products have a vulnerability of unrestricted upload of file. After obtaining the permissions of administrators, by sending a specific crafted packet to the vulnerable interface, an attacker can upload arbitrary files.
Severity：High
Base Score：8.7(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H)

6.**CVE-2022-45428**：

Some Dahua software products have a vulnerability of sensitive information leakage. After obtaining the permissions of administrators, by sending a specific crafted packet to the vulnerable interface, an attacker can obtain the debugging information.
Severity：Medium
Base Score：4.9(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N)

7.**CVE-2022-45429**：

Some Dahua software products have a vulnerability of server-side request forgery (SSRF). An Attacker can access internal resources by concatenating links (URL) that conform to specific rules.
Severity：Critical
Base Score：9.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

8.**CVE-2022-45430**：

Some Dahua software products have a vulnerability of unauthenticated enable or disable SSHD service. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could enable or disable the SSHD service.
Note: This vulnerability affects Linux based system only.
Severity：Medium
Base Score：5.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)

9.**CVE-2022-45431**：

Some Dahua software products have a vulnerability of unauthenticated restart of remote DSS Server. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could unauthenticated restart of remote DSS Server.

Note: This vulnerability affects Linux based system only.

Severity： High

Base Score： 8.6(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

10.**CVE-2022-45432**：

Some Dahua software products have a vulnerability of unauthenticated search for devices. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could unauthenticated search for devices in range of IPs from remote DSS Server.

Note: This vulnerability affects Windows based system only.

Severity： Medium

Base Score： 5.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N)

11.**CVE-2022-45433**：

Some Dahua software products have a vulnerability of unauthenticated traceroute host from remote DSS Server. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could get the traceroute results.

Note: This vulnerability affects Windows based system only.

Severity： Medium

Base Score： 5.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N)

12.**CVE-2022-45434**：

Some Dahua software products have a vulnerability of unauthenticated un-throttled ICMP requests on remote DSS Server. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could exploit the victim server to launch ICMP request attack to the designated target host.

Note: This vulnerability affects Windows based system only.

Severity： Medium

Base Score： 5.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)

Support Resources

For any cybersecurity questions or concerns related to Dahua products and solutions, please contact Dahua Cybersecurity Center(DHCC) at Cybersecurity@dahuatech.com. Dahua sincerely thank all of you for your efforts to our products security.