Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

16 December 2024

PIN Number

20241216-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP: CLEAR**

Please contact your local FBI field office with any questions related to this Private Industry Notification.

www.fbi.gov/contact-us/field-offices

HiatusRAT Actors Targeting Web Cameras and DVRs

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification (PIN) to highlight HiatusRAT[1] scanning campaigns against Chinese-branded web cameras and DVRs. Private sector partners are encouraged to implement the recommendations listed in the "Mitigation" column of the table below to reduce the likelihood and impact of these attack campaigns.

Threat

HiatusRAT is a Remote Access Trojan (RAT) whose latest iteration has likely been employed since July 2022. Malicious cyber actors commonly use RATs to take over and control a targeted device from a distance. The Hiatus campaign originally targeted outdated network edge devices. Cybersecurity companies have also observed these actors using the malware to target

[1] (U) Previous HiatusRAT campaigns have targeted edge routers to passively collect traffic and function as a covert network of command-and-control (C2) infrastructure.

a range of Taiwan-based organizations and to carry out reconnaissance against a US government server used for submitting and retrieving defense contract proposals.[2]

In March 2024, HiatusRAT actors conducted a scanning campaign targeting Internet of Things (IoT) devices in the US, Australia, Canada, New Zealand, and the United Kingdom. The actors scanned web cameras and DVRs for vulnerabilities including CVE-2017-7921, CVE-2018-9995, CVE-2020-25078, CVE-2021-33044, CVE-2021-36260, and weak vendor-supplied passwords. Many of these vulnerabilities have not yet been mitigated by the vendors. In particular, the actors targeted Xiongmai and Hikvision devices with telnet access. They used Ingram—a webcam-scanning tool available on Github—to conduct scanning activity. And they used Medusa—an open-source brute-force authentication cracking tool—to target Hikvision cameras with telnet access. Targeted TCP ports have included: 23, 26, 554, 2323, 567, 5523, 8080, 9530, and 56575.

The actors have demonstrated interest in the below CVEs, likely in furtherance of cyber exploitation efforts:

CVE	Description	Mitigation
CVE-2017-7921	An improper authentication occurs when an application does not adequately or correctly authenticate users. This may allow a malicious user to escalate privileges on the system and gain access to sensitive information. This issue has been discovered in the following Hikvision devices: DS-2CD2xx2F-I Series V5.2.0 Build 140721 to V5.4.0 Build 160530, DS-2CD2xx0F-I Series V5.2.0 Build 140721 to V5.4.0 Build 160401, DS-2CD2xx2FWD Series V5.3.1 Build 150410 to V5.4.4 Build 161125, DS-2CD4x2xFWD Series V5.2.0 Build 140721 to V5.4.0 Build 160414, DS-2CD4xx5 Series V5.2.0 Build 140721 to V5.4.0 Build 160421, DS-2DFx Series V5.2.0 Build 140805 to V5.4.5 Build 160928, and DS-2CD63xx Series V5.0.9 Build 140305 to V5.3.5 Build 160106.	**As of 13 December, 2024, Hikvision has not mitigated this vulnerability across all impacted devices**. Hikvision has released updates to mitigate the improper authentication vulnerability in cameras sold through authorized distributors. The updates can be found at: HSRC-201703-04
CVE-2018-9995	TBK DVR4104 and DVR4216 devices, as well as Novo, CeNova,	**There are currently no security updates to address these flaws.**

[2] https://blog.lumen.com/hiatusrat-take-little-time-off-in-a-return-to-action/

	QSee, Pulnix, XVR 5 in 1, Securus, Night OWL, DVR Login, HVR Login, and MDVR Login, which run re-branded versions of the original TBK DVR4104 and DVR4216 series, allow remote attackers to bypass authentication via a "Cookie: uid=admin" header, as demonstrated by a device.rsp?opt=user&cmd=list request that provides credentials within JSON data in a response.	Users should immediately replace vulnerable surveillance systems with actively supported models.
CVE-2020-25078	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure.	**Some affected devices are end-of-life devices.** Updates for affected firmware that is still supported can be found at: SAP10180
CVE-2021-33044	An identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypass device identity authentication by constructing malicious data packets.	Dahua recommends downloading a patch or from its website, Download Center, or contacting Dahua technical support to upgrade to a newer version.
CVE-2021-36260	A command injection vulnerability in the web server of some Hikvision products. Due to the insufficient input validation, malicious cyber actors can exploit the vulnerability to launch a command injection attack by sending messages with malicious commands.	Users should download the updated firmware from Hikvision at: Security Advisories

Recommendations

The FBI recommends limiting the use of the devices mentioned in this PIN and/or isolating them from the rest of your network. Companies should also regularly monitor networks and employ best practices for cybersecurity, including the following:

- Review or establish security policies, user agreements, and patching plans to address threats posed by these and other malicious cyber actors.
- Patch and update operating systems, software, and firmware as soon as manufacturer updates are available. If devices are no longer supported by the manufacturer, consider removing them from your network.
- Regularly change network system and account passwords, and avoid re-using passwords for multiple accounts. Avoid using default passwords for these devices and/or weak passwords.
- Enforce a strong password policy, such as requiring strong and unique passwords for all password-protected accounts, changing default usernames and passwords, employing lock-out rules for failed login attempts, restricting the reuse of passwords, and requiring the secure storage of passwords.
- Require multi-factor authentication wherever possible.
- Implement security monitoring tools that log network traffic to establish baseline activity, and that enable detecting and addressing abnormal network activity, including lateral movement on a network.
- Capture and monitor remote access/Remote Desktop Protocol (RDP) logs and disable unused remote access/RDP ports.
- Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Capture and regularly audit administrative user accounts and configure access controls under the concept of least privilege. Account privileges should be clearly defined and regularly reviewed and adjusted as necessary.
- Capture and regularly audit logs to ensure new accounts are legitimate users and to baseline legitimate user activity.
- Scan network for open and listening ports, and mediate those that are unnecessary.

- Identify and create offline backups for critical assets.
- Implement network segmentation wherever possible. If physical network segmentation cannot be accomplished, consider logical segmentation.
- Automatically update antivirus and anti-malware solutions and conduct regular virus and malware scans.

Report any suspected indications of compromise (IOC) to your local FBI field office or to the FBI's Internet Crime Complaint Center (IC3.gov). Locations and contact information for FBI field offices can be found at www.fbi.gov/contact-us/field-offices.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact

Administrative Note

This product is marked TLP: CLEAR. Subject to standard copyright rules, the information in this product may be shared without restrictions.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey