CYBER ADVISORY

TLP:CLEAR
4 November 2024

Critical Zero-day Vulnerability in PTZ Cameras

PTZoptics | OS Compromise | Bypass Security | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two critical vulnerabilities known as CVE-2024-8956[1] and CVE-2024-8957.[2] These two vulnerabilities affect PTZOptics PT30X-SDI/NDI-xx models with firmware versions prior to 6.3.40. When exploited together, they allow an unauthenticated attacker to execute remote code with operating system (OS)-level privileges, gaining full control over the system.[3] CVE-2024-8956, with a CVSS 3.x of 9.1, introduces insufficient authentication to /cgi-bin/param.cgi when requests are sent without a HTTP Authorization header. This can lead to an adversary leaking sensitive data such as usernames, password hashes, and configuration details. Additionally, the attacker can update individual configuration values or overwrite the whole file. CVE-2024-8957, with a CVSS 3.x of 9.8, enables an attacker to execute arbitrary OS commands by exploiting the camera's insufficient validation of the ntp_addr value when the ntp_client is started. A technical deep dive for these CVE's and a proof of concept is available.[4]

The Cal-CSIC recommends immediately updating to the latest PTZoptics firmware version.

For further information on applying updates please refer to PTZoptics Documentation.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] National Vulnerability Database; "CVE-2024-8956 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-8956; accessed 4 November 2024

[2] National Vulnerability Database; "CVE-2024-8957 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-8957; accessed 4 November 2024

[3] Bleeping Computer; "Hackers target critical zero-day vulnerability in PTZ cameras" https://www.bleepingcomputer.com/news/security/hackers-target-critical-zero-day-vulnerability-in-ptz-cameras/; accessed 4 November 2024

[4] GreyNoise; "GreyNoise Intelligence Discovers Zero-Day Vulnerabilities in Live Streaming Cameras with the Help of AI" https://www.labs.greynoise.io/grimoire/2024-10-31-sift-0-day-rce/; accessed 4 November 2024