

CVE-2024-8956

PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability

CISA KEV since Nov 4, 2024

Actively exploited

PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40 is vulnerable to an insufficient authentication issue. The camera does not properly enforce authentication to /cgi-bin/param.cgi when requests are sent without an HTTP Authorization header. The result is a remote and unauthenticated attacker can leak sensitive data such as usernames, password hashes, and configurations details. Additionally, the attacker can update individual configuration values or overwrite the whole file.

EVRS 76₁₀₀ Urgent priority	CVSS V3.1 9.1 Critical · NVD	EPSS 0.588 99.11st percentile · FIRST	CISA DEADLINE Nov 25, 2024 KEV since 2024 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.588 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
pt30x-sdi firmware	< 6.3.40	6.3.40	NVD
pt30x-ndi-xx-g2 firmware	< 6.3.40	6.3.40	NVD
pt30x-sdi	—	no fixed version listed	NVD
pt30x-ndi-xx-g2	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-58rw-8pf6-2mgq
NVD nvd.nist.gov/vuln/detail/CVE-2024-8956

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-49505

Additional guidance ptzoptics.com/firmware-changelog/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2024-8956

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.