> Podatności w oprogramowaniu kamery Vivotek IP7137

09 stycznia 2026 | CERT Polska(../../../../author/cert-polska/) | #podatność(../../../../tag/podatnosc/), #ostrzeżenie(../../../../tag/ostrzezenie/), #cve(../../../../tag/cve/)

CVE ID	CVE-2025-66049(https://www.cve.org/CVERecord?id=CVE-2025-66049)
Data publikacji	09 stycznia 2026
Producent podatnego oprogramowania	Vivotek
Nazwa podatnego oprogramowania	IP7137
Podatne wersje	0200a
Typ podatności (CWE)	Missing Authentication for Critical Function (CWE-306(https://cwe.mitre.org/data/definitions/306.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

CVE ID	CVE-2025-66050(https://www.cve.org/CVERecord?id=CVE-2025-66050)
Data publikacji	09 stycznia 2026
Producent podatnego oprogramowania	Vivotek
Nazwa podatnego oprogramowania	IP7137

Podatne wersje	0200a
Typ podatności (CWE)	Use of Default Password (CWE-1393(https://cwe.mitre.org/data/definitions/1393.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

CVE ID	CVE-2025-66051(https://www.cve.org/CVERecord?id=CVE-2025-66051)
Data publikacji	09 stycznia 2026
Producent podatnego oprogramowania	Vivotek
Nazwa podatnego oprogramowania	IP7137
Podatne wersje	0200a
Typ podatności (CWE)	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22(https://cwe.mitre.org/data/definitions/22.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

CVE ID	CVE-2025-66052(https://www.cve.org/CVERecord?id=CVE-2025-66052)
Data publikacji	09 stycznia 2026
Producent podatnego oprogramowania	Vivotek
Nazwa podatnego oprogramowania	IP7137
Podatne wersje	0200a
Typ podatności (CWE)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78(https://cwe.mitre.org/data/definitions/78.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

Opis podatności

CERT Polska otrzymał zgłoszenie o podatnościach w oprogramowaniu kamery Vivotek IP7137 i koordynował proces ujawniania informacji.

Ostrzeżenia(https://moje.cert.pl/komunikaty/)

Podatność CVE-2025-66049(https://www.cve.org/CVERecord?id=CVE-2025-66049): Kamera Vivotek IP7137 umożliwia dostęp do obrazu na żywo za pośrednictwem protokołu RTSP na porcie 8554 bez uwierzytelnienia. Pozwala to nieuprawnionym użytkownikom z dostępem sieciowym do kamery na podgląd obrazu, co może prowadzić do naruszenia prywatności i bezpieczeństwa użytkownika.

Podatność CVE-2025-66050(https://www.cve.org/CVERecord?id=CVE-2025-66050): Kamera Vivotek IP7137 domyślnie nie wymaga podania hasła podczas logowania na konto administratora. Chociaż możliwe jest ustawienie takiego hasła, użytkownik nie jest informowany o konieczności jego konfiguracji.

Podatność CVE-2025-66051(https://www.cve.org/CVERecord?id=CVE-2025-66051): Kamera Vivotek IP7137 jest podatna na atak typu path traversal. Uwierzytelniony atakujący może uzyskać dostęp do zasobów znajdujących się poza katalogiem webroot przy użyciu bezpośredniego żądania HTTP.

Podatność CVE-2025-66052(https://www.cve.org/CVERecord?id=CVE-2025-66052): Kamera Vivotek IP7137 jest podatna na atak typu command injection. Parametr `system_ntpIt` wykorzystywany przez endpoint `/cgi-bin/admin/setparam.cgi` nie jest odpowiednio filtrowany, co umożliwia użytkownikowi z uprawnieniami administratora przeprowadzenie ataku.

Producent nie odpowiedział na zgłoszenie CNA. Możliwe, że podatność dotyczy wszystkich wersji oprogramowania układowego (testowana wersja to 0200a). Ponieważ produkt osiągnął fazę End-Of-Life, nie należy oczekiwać wydania poprawki.

Podziękowania

Za zgłoszenie podatności dziękujemy Szymonowi Paszunowi.

Więcej o procesie zgłaszania podatności można przeczytać na stronie https://cert.pl/cvd/(https://cert.pl/cvd/).

CERT Polska
w social mediach

Facebook(https://www.facebook.com/CERT.Polska/)

Kontakt

ul. Kolska 12, 01-045 Warszawa
ePUAP: /NASK-Instytut/SkrytkaESP
e-Doręczenia: AE:PL-60057-61611-BCEGR-11

(/)

CERT Polska to zespół działający w strukturach NASK - Państwowego Instytutu Badawczego, powołany w 1996 roku do reagowania na incydenty bezpieczeństwa komputerowego. Realizuje zadania CSIRT NASK, jednego z trzech takich zespołów działających na poziomie krajowym w ramach krajowego systemu cyberbezpieczeństwa.

X(https://x.com/CERT_Polska)

Ostrzeżenia(https://moje.cert.pl/komunikaty/)

LinkedIn(https://www.linkedin.com/showcase/cert-polska)

GitHub(https://github.com/CERT-Polska)

e-mail: info@cert.pl(mailto:info@cert.pl)
Zgłaszanie incydentów:
incydent.cert.pl(https://incydent.cert.pl/)
cert@cert.pl(mailto:cert@cert.pl)

(../../../../en/posts/2026/01/CVE-2025-66049/) (/szukaj)

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”