

Kamery, ktoré testovala polícia obsahujú skryté čísla z Ruska a nezdokumentované mobilné pripojenie

21.8.2026 - | Slovensko.Digital

Analýza NBÚ odhalila závažné bezpečnostné nedostatky kamier NERO R-ONE nasadených ministerstvom vnútra. Slovensko.Digital považuje tento stav za vážne zlyhanie kontrolných mechanizmov štátu.

Národný bezpečnostný úrad (NBÚ) vykonal analýzu kamier NERO R-ONE, ktoré ministerstvo vnútra SR (MV SR) testovalo na kontrolu dopravy vo verejných priestoroch. Zistenia analýzy považuje Slovensko.Digital za mimoriadne závažné.

Kamery obsahujú nezdokumentovaný modul 3G/4G, ktorý vytvára samostatný komunikačný kanál nezávislý od siete, do ktorej je zariadenie zapojené. Firewall ani segmentácia siete tento kanál nevidia a nedokážu ho zablokovať. SIM kartu pritom môže do kamery vložiť ktokoľvek s fyzickým prístupom cez ľahko prístupný kryt, bez toho, aby sa dostal do záberu kamery.

Kľúčové zistenia NBÚ:

- Zariadenie obsahuje viaceré, aj nezdokumentované komunikačné schopnosti, predovšetkým:
 - aktívne vysielajúcu sieť Wi-Fi na lokálne pripojenie ku kamere,
 - nezdokumentovaný dodatočný modul 3G/4G (aj so zohľadnením dokumentácie výrobcu SIMICON) - v skúmanej vzorke bez vlozenej SIM karty,
 - súbor dvanástich konkrétnych zabudovaných telefónnych čísel s prefixmi +78 a +79, teda z Ruskej federácii. Ak je vložená SIM karta, SMS správa prijatá z niektorého z týchto čísel umožňuje pri znalosti vstavaného hesla získať plný administrátorský prístup ku kamere, ako aj sieťový prístup ku kamere a k sieťam, ktoré sú k nej pripojené,
 - používateľské rozhranie s nakonfigurovaným RTSP streamom, ktorý bez hesla sprístupňuje obsah z kamery komukoľvek so sieťovým pripojením.
- Softvér kamery obsahuje viaceré bezpečnostné zraniteľnosti.
- Zariadenie umožňuje prihlásenie do zabudovaného administrátorského účtu "root" z konzoly (pri fyzickom prístupe k zariadeniu), ako aj po sieti prostredníctvom protokolov Telnet a SSH. Ide o prihlásenie do operačného systému, ktoré je nezávislé od prihlásenia do webového konfiguračného rozhrania kamery a umožňuje úplné ovládanie zariadenia. Používateľský účet root má vo firmvéri napevno definované heslo.

"Zariadenia s takýmito vlastnosťami by sa nemali dostať ani len do testovacej prevádzky žiadneho štátneho systému. Že sa tak stalo, naznačuje vážne zlyhanie kontrolných mechanizmov ministerstva vnútra. Obzvlášť znepokojujúci je nezdokumentovaný 3G/4G modul - ide o komunikačný kanál, ktorý štát jednoducho nevidí a nemôže kontrolovať," dodáva eGov expert Peter Hanečák zo Slovensko.Digital.

Slovensko.Digital odporúča MV SR neodkladne analyzovať zlyhanie kontrolných mechanizmov, ktoré umožnili nasadenie týchto zariadení do testovacej prevádzky. Zároveň odporúča vykonať audit všetkých existujúcich kamerových systémov ministerstva a overiť, či neobsahujú obdobné zraniteľnosti.

Kamerové systémy predstavujú výrazný zásah do súkromia občanov. Polícia má síce k dispozícii osobitné právomoci a výnimky, ich využívanie si však vyžaduje zodpovedajúcu odbornú starostlivosť. Tá v tomto prípade zjavne chýbala.

<https://slovensko.digital/kamery-ktore-testovala-policia-obsahuju-skryte-cisla-z-ruska-a-nezdokumentovane-mobilne-pripojenie>