VIVOTEK Cyber Security Announcement

VIVOTEK has issued this cyber security notice in response to two vulnerabilities identified in VIVOTEK cameras. CVE-2017-9828, and CVE-2017-9829, describe methods an attacker with admin access to a camera can use to expose files or other data contained within the camera. Both vulnerabilities rely on the attacker having Administrator privilege to exploit. Systems with no root password set, or a root password that is easily guessed are at significant risk. If a strong password is used for the root account, the risk of these two vulnerabilities is greatly reduced. This announcement lists action items for our partners to follow for cyber security matters.

VIVOTEK Actions:

- VIVOTEK strongly recommends that users set up a Root Password and create a strong password immediately to safeguard your VIVOTEK device from high risk. Users are welcome to follow the instructions on page 6 of the VIVOTEK Security Hardening Guide officially released on January 3rd, 2017.
- CVE -2017-9828 & CVE -2017-9829: VIVOTEK will release firmware updates for affected models before July 20th, 2017. Users can download the new firmware from VIVOTEK Downloads and upgrade their cameras to solve this issue. Please be assured solving this issue is our top priority.
- VIVOTEK's new products will by default ask users to set up the Password as a required step to reduce cyber security vulnerabilities.
- For any concerns on VIVOTEK cyber security, you can reach us at cybersecurity@vivotek.com

We also encourage users to take advantage of our many online resources:

- VIVOTEK Downloads: With useful materials, such as brochures, firmware/software updates.
- VIVOTEK Support: Including Top FAQ, Technical Videos, and Security Hardening Guide for efficient online assistance.
- VIVOTEK Customer Community: To obtain assistance from the VIVOTEK technical support team, you can register online with our customer community and engage more with VIVOTEK's solutions and services.

VIVOTEK Inc.
July 7th, 2017