VIVOTEK Vulnerability Policy

1. Overview

Cyber attacks are a part of the current atmosphere of network computing devices. Due to this unfortunate reality, VIVOTEK pushes forth with industry best practices in order to reduce security vulnerabilities in our products.

VIVOTEK cyber security assurance efforts are built into the lifecycle of its products, including development, verification, manufacturing, delivery and service. We are constantly evaluating and enhancing our cyber security efforts in order to provide our valued customers with the highest quality and most reliable products. Although VIVOTEK cannot protect standardized network protocols and services from cyber attacks, we are committed to helping minimize and stop such events on our customers and VIVOTEK products.

For the latest VIVOTEK software and firmware updates, please visit https://www.vivotek.com/website/firmware. Here you will find the latest security patches for current VIVOTEK products.

2. Vulnerability management

VIVOTEK is always working to maintain the highest level of security for our products and customers. Based on the risk for users when products are deployed, and used in a recommended way, we classify the severity of vulnerabilities as either critical or non-critical. We release firmware updates on a regular schedule to fix bugs/non-critical vulnerabilities that are found in our products. If the occasion arises where a new critical vulnerability is discovered that leaves our devices highly vulnerable to attack, then VIVOTEK will focus priorities to fix this issue immediately outside of the regular schedule.

For the most up to date security advisory, please go to https://www.vivotek.com/cybersecurity/ There you will find a description and summary of the vulnerability, our recommendation, and plan of action to neutralize the threat.

3. Reporting vulnerabilities

If you find a security vulnerability in VIVOTEK products, please do not hesitate to report the

problem. We encourage any/all end users, resellers, integrators, VMS partners, and all customers that find a vulnerability to update VIVOTEK, and help us resolve & eliminate these threats. Please contact us at security@vivotek.com to report a vulnerability or other security concern.

Please check https://www.vivotek.com/cybersecurity/ before contacting the team as your concern may already have been processed in a security advisory.

For other support issues, please contact technical@vivotek.com

4. Response process

VIVOTEK will analyze all submissions to security@vivotek.com, acknowledge and reply within 72 hours, and if needed ask more questions to help in identifying a resolution. VIVOTEK may also post the newly identified vulnerability to https://www.vivotek.com/cybersecurity/

5. Receiving information from VIVOTEK

VIVOTEK publishes this policy, security hardening guide, security advisories and statements on https://www.vivotek.com/cybersecurity/

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.