

Advisory on VIVOTEK Camera Firmware Vulnerability



A vulnerability in VIVOTEK camera firmware could allow remote command execution, potentially compromising the camera system. Institutions using affected models should take immediate action to mitigate risks.

- VIVOTEK camera firmware has a vulnerability allowing remote command execution.
- Affected models include various V and C Series cameras.
- Successful exploitation can lead to full compromise of the camera system.
- Immediate action is recommended for institutions using these devices.

Overview

VIVOTEK has reported a critical vulnerability in its camera firmware that could enable attackers to execute commands remotely, potentially gaining root access and fully compromising the camera system. This affects

multiple models across the V and C Series.

Affected Models

The vulnerability impacts the following VIVOTEK camera models: V Series FD9187, FD9189, FD9365, FD9387, FD9389, FD9391, FE9180, FE9191, FE9382, FE9391, IB9365, IB9387, IB9389, IB939, IP9165, IP9171, IP9172, IP9181, IP9191, IT9389, MA9321, MA9322, MS9321, among others. Institutions using these models should assess their exposure.

Recommended Actions

To mitigate the risks associated with this vulnerability, institutions should take the following actions:

- Review the list of affected VIVOTEK camera models in use.
- Update the firmware of affected devices to the latest version provided by VIVOTEK.
- Implement network segmentation to limit access to camera systems.
- Monitor network traffic for unusual activity related to camera devices.
- Conduct a security audit of camera systems to identify potential vulnerabilities.

What to do now

1. Review the list of affected VIVOTEK camera models in use.
2. Update the firmware of affected devices to the latest version provided by VIVOTEK.
3. Implement network segmentation to limit access to camera systems.
4. Monitor network traffic for unusual activity related to camera devices.
5. Conduct a security audit of camera systems to identify potential vulnerabilities.