VIVOTEK
A Delta Group Company

VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2026-01

CVE ID: CVE-2026-1642

First Published: April 17, 2026

Last Update: July 24, 2026

Status: Confirmed

Revision: 1.0

Executive Summary

VIVOTEK has reviewed CVE-2026-1642, a NGINX vulnerability related to SSL/TLS (TLS (Transport Layer Security) is the modern, secure version of SSL.) upstream handling. Based on VIVOTEK's technical assessment, the risk to affect VIVOTEK surveillance camera products is considered limited under standard deployment conditions. "CVE-2026-1642 is about how NGINX handles upstream connections, and it only occurs when the upstream communication uses TLS (HTTPS)."

In VIVOTEK embedded camera products, the built-in NGINX server is primarily used as a reverse proxy for communication between internal modules. These internal communication paths generally use localhost, IPC, or Unix domain sockets rather than external TLS (HTTPS) upstream connections. As a result, the specific attack conditions required for CVE-2026-1642 are generally not present in VIVOTEK's evaluated product architecture.

VIVOTEK will continue to maintain product security through regular firmware maintenance. For products on the active track platform, NGINX version updates will be scheduled in release 2603 or later. For long-term support platform products, no corresponding NGINX update is currently planned.

Overview:

CVE-2026-1642 is associated with SSL/TSL(HTTPS) upstream injection behavior in NGINX. The vulnerability is relevant only when NGINX is configured to proxy requests to an HTTPS upstream server and an attacker is able to position a man-in-the-middle attack between NGINX and that upstream connection.

VIVOTEK's evaluation indicates that, in current camera implementations, NGINX is used mainly to connect internal services within the device. These communications are typically implemented using localhost, IPC, or Unix domain sockets, and therefore do not enter the external SSL/TSL(HTTPS) upstream scenario required for this vulnerability.

Even in exceptional internal deployment scenarios where HTTPS may be used between internal components, successful exploitation would still require attacker control over a privileged internal communication path. In practice, this would imply a level of system compromise that already provides broader control over the device, limiting the practical impact of this specific vulnerability.

Accordingly, VIVOTEK considers CVE-2026-1642 not applicable in the evaluated standard deployment scenario for the products covered by this advisory.

Affected Products:

VIVOTEK has confirmed that NGINX was officially introduced into firmware starting from release 2303. Therefore, this advisory applies only to products using NGINX-based firmware (2303 or later). Products using firmware versions prior to 2303 are based on BOA and are not affected by CVE-2026-1642.

Affected products are classified into the following categories:

- Active track platform
- Long-term support platform

The complete product list is provided in Appendix A.

Workaround:

No specific workaround is required for products operating under the evaluated standard deployment scenario.

As a general security practice, NGINX should not be configured to proxy requests to external SSL/TLS (HTTPS) upstream endpoints unless such use is explicitly required, reviewed, and secured as part of the product design.

Solution:

For active track platform models, NGINX version updates will be scheduled as part of regular firmware maintenance in release 2603 or later.

For long-term support platform models, no NGINX version update is planned, because the vulnerability is assessed as not applicable under the current deployment scenario, and the overall impact is considered limited.

Revision History:

Revision	Date	Description
0.1	2026/4/17	Initial draft
1.0	2026/7/24	First published

Appendix A. Complete Product List

A.1 Active track platform

Form Factor	Camera Models
Fixed Dome	FD9399-H, FD9399-EHV, FD9399-EHTV, FD9189-H-V3, FD9389-EHV-V3, FD9389-EHTV-V3, FD9365-EHTV-v2, FD9391-EHTV-v2, FD9187-HT-V3, FD9387-EHTV-V3, FD9383-HV, FD9383-HTV, VFD04A
Bullet	IB9399-EHV, IB9399-EHTV, IB9389-EHV-V3, IB9389-EHTV-V3, IB9365-EHTV-v2, IB9391-EHTV-v2, IB9387-EHTV-V3, IB9383-HV, IB9383-HTV, VIB04A-W
Box	IP9181-HT-v2, IP9191-HT-v2 (i-CS Lens), IP9191-HT-v2 (Non i-CS Lens), IP9191-LPC-v2 (i-CS Lens), IP9191-LPC-v2 (Non i-CS Lens)
Turret	IT9389-HTVW-V3, IT9399-HTVW, IT9383-HVW, IT9383-HTVW, IT9399-HVW, IT9389-HVW-V3, VIT04A-W
Panoramic	CC9381-HV-V2, CC9380-HV-V2, CC9391-HV, CC9390-HV, MA9311-EHTV, MA9312-EHTV, MA9322-EHTV-V2
360° Fisheye	FE9191-H-v2 (1.18mm), FE9192-H, FE9391-EHV-V2 (1.18mm), FE9391-EV-V2-M12, FE9391-EV-V2-M12(M)
Speed Dome	SD9394-EHL, SD9387-EHL, SD9367-EHL

A.2 Long-term support platform

Form Factor	Camera Models
Fixed Dome	FD9167-HT-v2, FD9189-HT-v2, FD9189-H-v2, FD9367-EHTV-v2, FD9389-EHTV-v2, FD9389-EHV-v2, FD9369
Bullet	IB9367-EHT-v2, IB9389-EHT-v2, IB9389-EH-v2, IB9369
Box	IP9165-HT-v2 (i-CS Lens), IP9165-HT-v2 (non i-CS Lens), IP9165-LPC-v2 (i-CS Lens), IP9165-LPC-v2 (Non i-CS Lens)
Turret	IT9389-H-v2
Panoramic	MS9321-EHV-V2, MS9390-EHV-V2
360° Fisheye	FE9382-EHV-v2
Mobile Dome	MD9582-H, MD9584-H
Corner Dome	CD9381-HNTV, CD9381-HNVF2
Speed Dome	SD9368-EHL, SD9384-EHL, SD9161-H-v2
Split-Type	VC9101 [CU9171], VC9101 [CU9183]