VIVOTEK
A Delta Group Company

VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2026-02

CVE ID: CVE-2026-43284

First Published: April 17, 2026

Last Update: September 1, 2026

Status: Confirmed

Revision: 1.0

Executive Summary

Overview:

CVE-2026-43284, commonly referred to as "Dirty Frag" or "Copy Fail 2", is a critical local privilege escalation (LPE) vulnerability affecting the Linux kernel. Discovered by security researcher Hyunwoo Kim (@v4bel), the flaw resides in the interaction between the network socket buffer (skb) fragmentation subsystem and the Encapsulating Security Payload (ESP) processing mechanism. The vulnerability allows an unprivileged local attacker to execute arbitrary writes against memory pages mapped to the system's page cache.

The core of the issue is a missing state flag when the kernel handles the MSG_SPLICE_PAGES directive during IPv4 and IPv6 datagram appending. This directive attaches data from a pipe directly to a socket's buffer without executing a copy operation. If the source of the pipe is a file, the resulting socket buffer fragments reference the Linux page cache directly. The kernel fails to properly mark these fragments as shared memory.

The vulnerability is classified under CWE-123 (Write-what-where Condition) and CWE-787 (Out-of-bounds Write). By exploiting the lack of copy-on-write enforcement during ESP decryption, an attacker can modify the contents of any file they have read access to. This directly undermines the operating system's permission model and facilitates complete system compromise.

VIVOTEK
A Delta Group Company

Affected Products:

Product Category	Number of Affected Models	Camera Models	Fixed FW Version / Status
Vortex Camera	**15**	**IT839-H** **IB839-EHT** **IB839-EH** **FD839-EHTV** **FD839-EHV** **FD819-HT** **FD819-H** **CC831-HV** **CC830-HV** **MS930-EHV** **FE931-EHV** **FE912-H** **IB837-HT** **FD837-HTV** **SD834-EHL**	**27.1.0**
Fixed Dome / Bullet / Turret Cameras	**10**	**FD9167-HT-v2** **FD9189-HT-v2** **FD9189-H-v2** **FD9367-EHTV-v2** **FD9389-EHTV-v2** **FD9389-EHV-v2** **IB9367-EHT-v2** **IB9389-EHT-v2** **IB9389-EH-v2** **IT9389-H-v2**	**No planned fix** Most models are EOL, and this CVE is not used by the product application.
Fixed Dome / Bullet / Box / Compact Cameras	**16**	**FD9365-EHTV-v2** **FD9391-EHTV-v2** **FD9187-HT-V3** **FD9387-EHTV-V3** **IB9365-EHTV-v2** **IB9391-EHTV-v2** **IB9387-EHTV-V3** **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)** **CC9381-HV-V2**	**2701**

		CC9380-HV-V2 **CC9391-HV** **CC9390-HV**	
Box Camera	**1**	**IP9181-LPC-v2**	**2701**
Box / Mobile / Split-type Cameras	**8**	**IP9165-LPC-v2 (i-CS Lens)** **IP9165-LPC-v2 (Non i-CS Lens)** **MD9582-H** **MD9584-H** **VC9101 [CU9171]** **VC9101 [CU9183]** **MD8564-EH-V2** **MD8564-DEH-V2**	**2403**
Fisheye Cameras	**5**	**FE9191-H-v2 (1.18mm)** **FE9192-H** **FE9391-EHV-V2 (1.18mm)** **FE9391-EV-V2-M12** **FE9391-EV-V2-M12(M)**	**2701**
Speed Dome Cameras	**3**	**SD9394-EHL** **SD9387-EHL** **SD9367-EHL**	**2701**

Risk Assessment for EOL Models: For FD9167-HT-v2, FD9189-HT-v2, FD9189-H-v2, FD9367-EHTV-v2, FD9389-EHTV-v2, FD9389-EHV-v2, IB9367-EHT-v2, IB9389-EHT-v2, IB9389-EH-v2, and IT9389-H-v2, no firmware modification is planned because most of these models have reached EOL and internal assessment indicates that this CVE is not used by the product application. The residual risk is assessed as limited under the condition that the affected kernel path or related feature is not exposed or used in the product scenario. However, because CVE-2026-43284 is classified as a high-severity local privilege escalation vulnerability, the decision should be documented with clear EOL status, product applicability analysis, and mitigation guidance for customers who continue operating these models.

Workaround:

* - ****Restrict Network Access (Network Isolation / ACL):**** Enable the device's built-in IP filter or configure Access Control Lists (ACLs) via an external firewall. Strictly limit access to the device, allowing connections only from trusted IP addresses (e.g., designated NVRs, VMS servers, or management jump hosts).

* - ****Enforce Strict Authentication Management:**** Disable the Guest account on the device and ensure that all administrator and user accounts use strong passwords. This prevents

attackers from gaining initial access via weak credentials.

Solution:

- Update to the latest firmware/software version immediately. Make Certain to back up device settings before applying the update.

- If an immediate update is not possible, do consider temporarily disabling the affected features or restricting network access.

Revision History:

Revision	Date	Description
0.1	April 17, 2026	Initial draft
1.0	September 1, 2026	First published