One Solution. One Company.

SN-14

CVE-2026-31431 / CVE-2026-43284 / CVE-2026-43500 Copy Fail, Dirty Frag Vulnerabilities

Version 1.0.0

1 Overview

This document has been prepared to provide a comprehensive impact analysis and an official technical response regarding the major security vulnerabilities recently reported in the Linux kernel environment: CVE-2026-31431 (Copy Fail), CVE-2026-43284 (Dirty Frag - xfrm/ESP variant), and CVE-2026-43500 (Dirty Frag - RxRPC variant), specifically concerning their impact on IDIS's hardware appliance product lines (NVRs and IP cameras)

2 Vulnerability Type & Impact

The detailed information and technical summaries of the vulnerabilities analyzed are as follows:

CVE Identifier	Alias	Vulnerability Type & Impact
CVE-2026-31431	Copy Fail	This vulnerability involves improper exception handling during specific data copying or file system/memory operations, which is known to potentially cause abnormal system termination or privilege escalation.
CVE-2026-43284	Dirty Frag (xfrm/ESP Variant)	This vulnerability arises during the network packet fragmentation (IP fragmentation) and reassembly process, which can induce memory corruption, potentially leading to Denial of Service (DoS) attacks or Remote Code Execution (RCE).
CVE-2026-43500	Dirty Frag (RxRPC Variant)	This variant vulnerability is based on the Remote Procedure Call (RxRPC) protocol and shares the underlying network fragmentation (Dirty Frag) logic flaw of the Linux kernel. It can induce memory corruption during specific protocol communications, potentially resulting in system privilege escalation or a Denial of Service (DoS).

3 Affected Products

No Impact.

4 Detailed Description (Rationale)

4.1 Common Security Architecture of IDIS Products

From the design phase, IDIS's NVR and IP camera product lines adopt a closed hardware appliance architecture to fundamentally block external threats. This common architecture completely neutralizes the penetration paths through which the aforementioned vulnerabilities could manifest.

4.1.1 Physical Security & Hardware Anti-Hacking Measures

- **Complete Block of Console Access:** Physical and logical console access interfaces, both internal and external to the product, have been completely removed and blocked, making it impossible to execute arbitrary commands through a direct connection to the device.

4.1.2 OS-Level Access Security & Network Daemon Control

- Strict Account Management & Authentication:
    - NVR Product Line: General user accounts do not exist within the system, and the root account is securely locked using cryptographic algorithms, rendering it completely inaccessible.
    - IP Camera Product Line: No general user accounts exist, and the system does not support any services or interfaces that allow access to the internal system shell using an account.
- Remote Interface Restriction: Network daemons that could be exploited for remote management or penetration (such as sshd, telnetd, rlogind, etc.) are strictly disabled at the kernel and OS levels, and the source code itself is entirely excluded from the system.
- Air-gapped Design: Engineered with a hardware structure that completely blocks all unauthorized access paths from both internal and external sources, making local and remote penetration scenarios structurally impossible.

5 Impact Analysis & Technical Rationale by Product Line

IDIS NVR Product Line (Standalone NVR Hardware Appliance)

CVE Identifier	Analysis Result	Evaluation Result
CVE-2026-31431 (Copy Fail)	**Not Applicable** **(No Impact)**	1. Although this vulnerability is a Local Privilege Escalation (LPE) bug, the IDIS common security architecture ensures that no local shell entry point exists through which unauthorized commands could be executed. 2. The 'Kernel Crypto Socket Interface' option, which is a mandatory prerequisite for this vulnerability to manifest, is entirely excluded at the build phase, fundamentally blocking the attack vector.
CVE-2026-43284 (Dirty Frag - xfrm)	**Not Applicable** **(No Impact)**	1. It is structurally secure as there is no local shell entry point through which unauthorized commands can be executed. 2. The 'Kernel Crypto Socket Interface' option is entirely excluded during the compilation phase. 3. By completely disabling the IPsec (xfrm) security policies and transformation engines across all network interfaces (disable_xfrm=1, disable_policy=1), any potential for real-time exploitation via external packets is doubly contained as part of a defense-in-depth strategy.
CVE-2026-43500 (Dirty Frag - RxRPC)	**Not Applicable** **(No Impact)**	1. The hardware structure is designed such that local penetration scenarios are completely non-viable. 2. The RxRPC subsystem is entirely disabled in the kernel compilation options, resulting in absolutely no impact from this variant vulnerability.

6 4.2. IDIS IPC (Network 카메라) 제품군

CVE Identifier	Analysis Result	Evaluation Result
CVE-2026-31431 **CVE-2026-43284** **CVE-2026-43500**	**Not Applicable** **(No Impact)**	1. In the IPC product line as well, the console and remote daemons (such as sshd, telnetd, etc.) are completely controlled at the OS level, making local shell access and unauthorized command execution impossible. 2. Since the system does not support any internal services that utilize user accounts, obtaining standard user privileges—which is a mandatory prerequisite for Local Privilege Escalation (LPE) vulnerabilities—is fundamentally impossible, thereby guaranteeing system security.

7 Conclusion & Recommendations

Comprehensive Analysis Summary

In conclusion, while the CVE-2026-31431, CVE-2026-43284, and CVE-2026-43500 vulnerabilities target Linux kernel-based Local Privilege Escalation (LPE), we officially confirm that IDIS NVR and IP camera product lines are entirely unaffected (secure). This is because the devices completely lack local or remote shell entry points for attacker penetration, and the mandatory kernel options and protocol subsystems required to trigger these vulnerabilities have already been disabled and excluded during the build phase.

8 References

[1] OpenCVE: https://app.opencve.io/cve/

Contact Us

Additional information may be updated in this document in the future. For any questions or concerns related to this issue, please email security@idisglobal.com.

Version History

Version	Writer	Revision Date	Remarks
1.0.0	Roy Lee	June 01. 2026	Initial Release