NATIONAL CSIRT-CY

Command Execution Vulnerability in **Hikvision Switch Products** **CVE-2026-3828**

11 May 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) has observed Hikvision has disclosed a high-severity authenticated remote command execution vulnerability affecting several discontinued smart switch products.

TECHNICAL DETAILS:

Hikvision has disclosed a high-severity authenticated remote command execution vulnerability affecting several discontinued smart switch products. The flaw arises from insufficient input validation mechanisms within the device firmware, enabling authenticated attackers to inject and execute arbitrary operating system commands remotely.

Vulnerability Details

- **CVE ID:** CVE-2026-3828
- **CVSS v3.1 Score:** 7.2 (High) (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
- **Impact:** Attackers with valid credentials can exploit this flaw by sending crafted packets containing malicious commands to affected devices, leading to arbitrary command execution.

Affected Versions and Fix

Product Model	Affected Versions	Fixed Version
DS-3E1310P-SI	Versions below and including V1.2.4_210623	V1.2.5_260309
DS-3E1318P-SI	Versions below and including V1.2.0_210823	V1.2.1_260309
DS-3E1326P-SI	Versions below and including V1.2.0_210823	V1.2.1_260309

RECOMMENDATIONS:

The Digital Security Authority (DSA) recommends immediately **upgrading** all affected devices to the latest fixed firmware versions immediately.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

1. https://www.hikvision.com/en/support/cybersecurity/security-advisory/command-execution-vulnerability-in-some-hikvision-switch-product/

DISCLAIMER:

The information presented in this report is based on available data up to the 11th of May 2026.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.