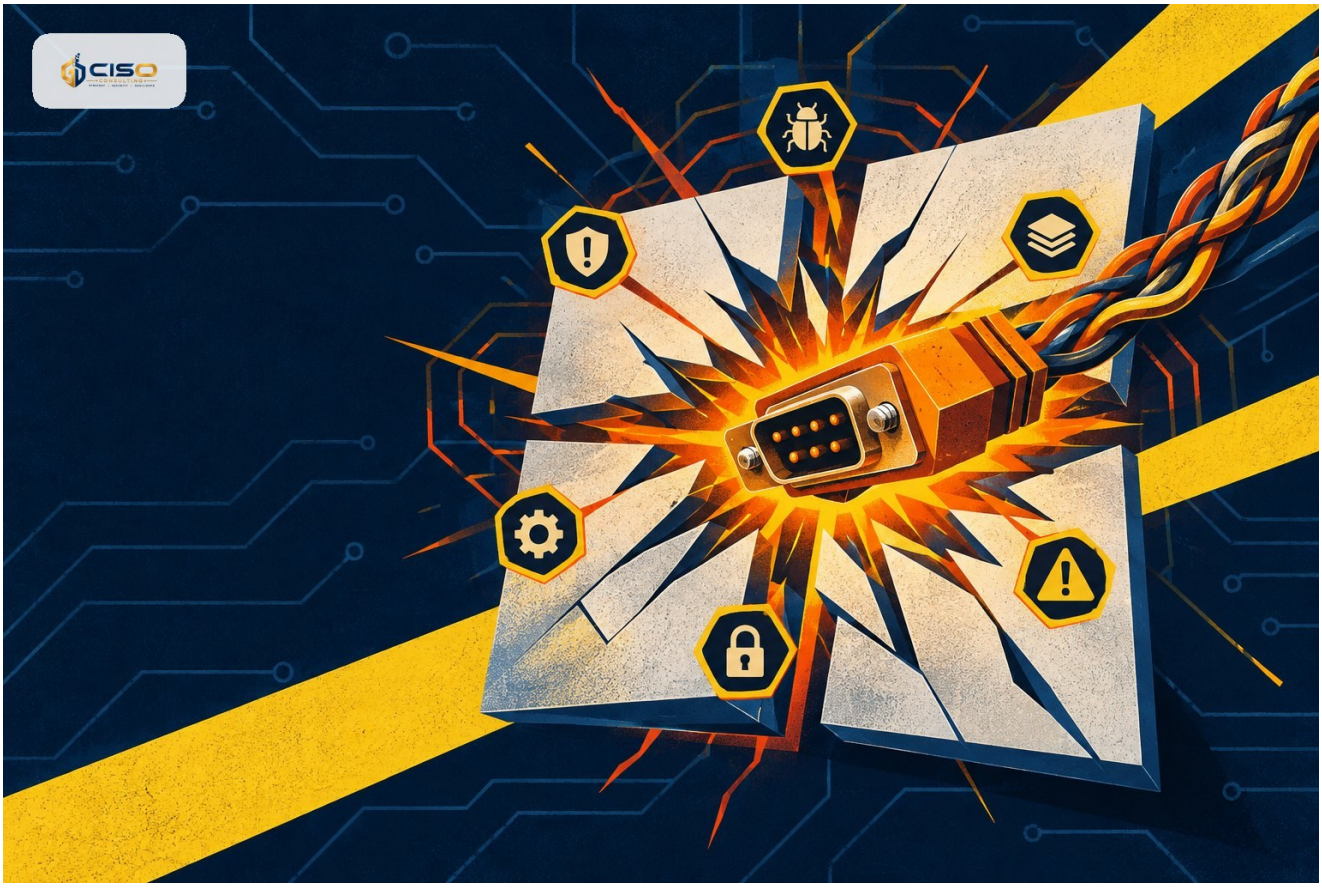
CISA flags kernel-crash flaws in HMS Networks PEAK-System PCAN Windows drivers



CISA published an advisory on PEAK-System PCAN Windows drivers from HMS Networks. Six CVEs could let exploitation crash the Windows kernel. The vendor equipment CVSS v3 score is 7.1.

- Successful exploitation could crash the Windows kernel.
- Affected: PEAK-System Device Driver Setup up to 5.1.2.1151 and PCAN Windows CAN device drivers up to 5.1.2.
- Six CVEs are listed: CVE-2026-109576, CVE-2026-101103, CVE-2026-94188, CVE-2026-103672, CVE-2026-110322 and CVE-2026-105960.
- Weakness types include out-of-bounds write, classic buffer overflow, improper array index validation, untrusted pointer dereference and length parameter inconsistency.

> - CISA lists sectors such as transportation, healthcare, energy and critical manufacturing; the vendor is headquartered in Sweden.

CISA has published an industrial control systems advisory covering PEAK-System PCAN drivers for Windows, distributed under HMS Networks. The advisory states that successful exploitation of the listed vulnerabilities could crash the Windows kernel.

What is affected

Two components are named: PEAK-System Device Driver Setup in versions up to and including 5.1.2.1151, and PCAN Windows CAN device drivers in versions up to and including 5.1.2. Both are associated with the same six CVEs: CVE-2026-109576, CVE-2026-101103, CVE-2026-94188, CVE-2026-103672, CVE-2026-110322 and CVE-2026-105960.

The weaknesses described are out-of-bounds write, classic buffer overflow, improper validation of an array index, untrusted pointer dereference and improper handling of length parameter inconsistency. The vendor equipment CVSS v3 score is 7.1. The first CVE entry describes a parser that detected a malformed record but still advanced its processed-bytes counter.

Why it matters

CISA lists transportation systems, healthcare and public health, energy and critical manufacturing as relevant sectors, with worldwide deployment. A kernel crash on a Windows host that talks to CAN hardware can interrupt engineering, test or monitoring workstations. The excerpt we reviewed does not state a fixed version or mitigations, so teams should read the full CISA advisory and the vendor's notes before acting.

What to do now

1. Inventory Windows hosts running PEAK-System Device Driver Setup or PCAN drivers, and record their versions.
2. Compare versions against the affected ranges: up to 5.1.2.1151 for the setup package and up to 5.1.2 for the drivers.
3. Read the full CISA advisory and HMS Networks or PEAK-System guidance for fixed versions and mitigations.
4. Restrict access to affected workstations to authorised users, and avoid exposing them to untrusted networks.
5. Include these hosts in OT and endpoint patch tracking under your OT cybersecurity governance.