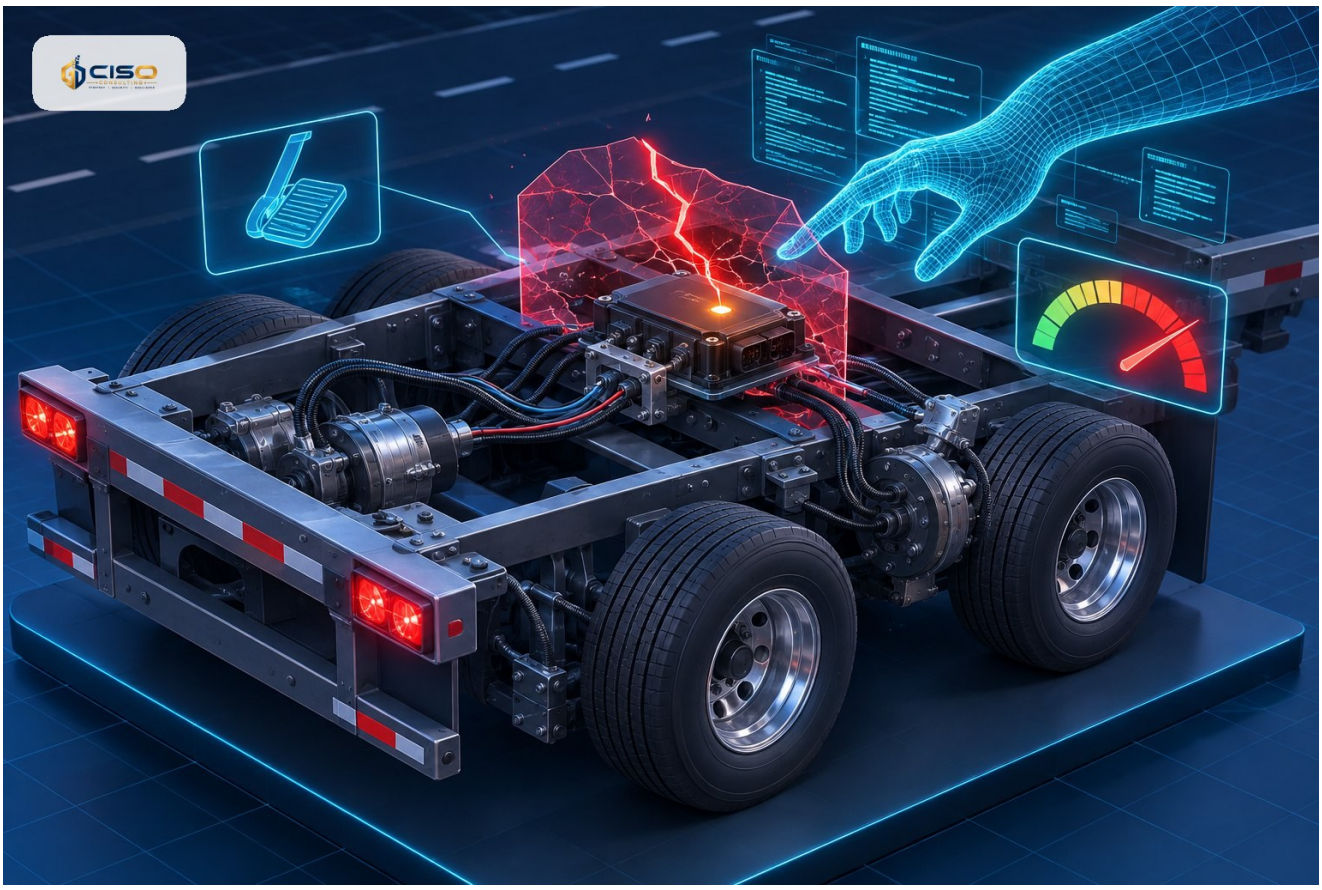
CISA flags critical flaws in Elecbrakes EB2, VM1 and ELBC2000 trailer brake controllers



CISA published an ICS advisory on three vulnerabilities in Elecbrakes EB2, VM1 and ELBC2000 trailer brake products, rated CVSS v3 9.6. Exploitation could allow control of trailer brakes and firmware changes.

- CVSS v3 score is 9.6; the advisory covers CVE-2026-124281, CVE-2026-125273 and CVE-2026-96805.
- Affected: EB2 up to 3.0.4.2.0, VM1 before 1.3.4.2.1, and all ELBC2000 versions.
- Weakness types: exposed dangerous method, capture-replay authentication bypass, and missing authentication for a critical function.
- Impact includes control of trailer brakes, firmware modification, disabled brake lights and altered brake conditions.

> - Deployment is listed as Australia and New Zealand; the vendor has released updated firmware.

CISA has released an industrial control systems advisory covering Elecbrakes EB2, VM1 and ELBC2000, products used in trailer braking. The advisory assigns a CVSS v3 score of 9.6 and lists three vulnerabilities: CVE-2026-124281, CVE-2026-125273 and CVE-2026-96805.

What is affected

The affected versions are EB2 up to and including 3.0.4.2.0, VM1 before 1.3.4.2.1, and all versions of ELBC2000. The three weaknesses are an exposed dangerous method or function, authentication bypass by capture-replay, and missing authentication for a critical function. One of them concerns an unprotected firmware-update channel that may allow unauthorized firmware modification.

According to CISA, successful exploitation could let an attacker take control of a trailer's brakes, modify firmware, disable brake lights, change brake conditions or disable other critical safety features.

Scope and vendor response

The advisory lists the transportation sector and notes deployment in Australia and New Zealand, with the vendor headquartered in Australia. Elecbrakes has released updated firmware. The source excerpt does not give details on exploitation in the wild or on a fix for ELBC2000.

What this means for Saudi organizations

Direct exposure is likely limited, given the stated deployment regions. Organizations in the Kingdom that operate imported trailers or mixed fleets, or that manage logistics and transport risk, should confirm whether these products are present and review supplier assurance for connected vehicle components.

What to do now

1. Check fleet and asset inventories for Elecbrakes EB2, VM1 and ELBC2000 units, including imported trailers.
2. Apply the vendor's updated firmware where available and confirm versions: EB2 above 3.0.4.2.0, VM1 at 1.3.4.2.1 or later.
3. For ELBC2000, contact the supplier for remediation guidance, as all versions are listed as affected.
4. Restrict physical and wireless access to firmware-update interfaces and log any update activity.
5. Add connected vehicle components to OT and third-party risk reviews and record the outcome.