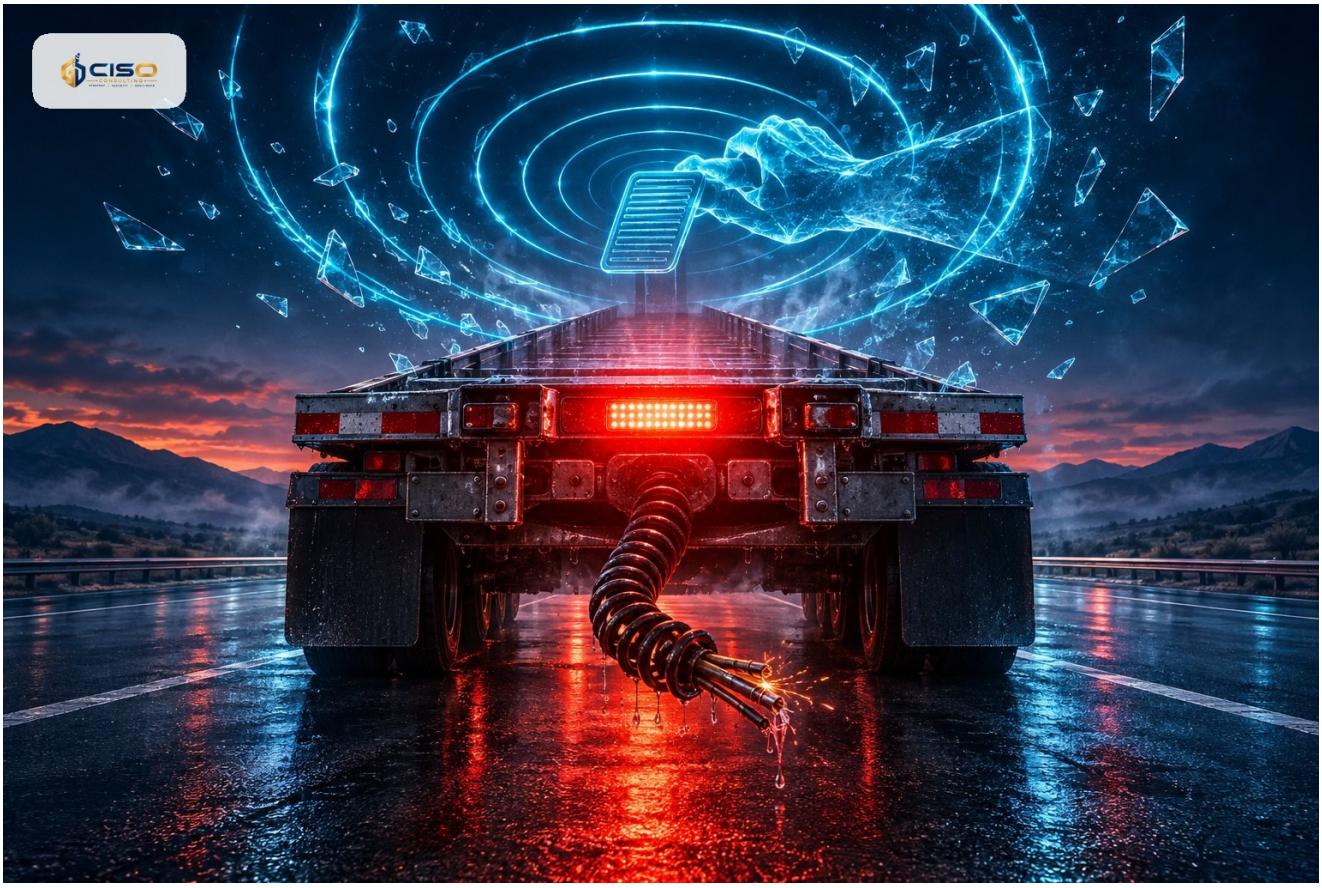
# Elecbrakes Bluetooth Flaws Let Nearby Attackers Trigger Trailer Brakes



Researchers found Bluetooth flaws in Elecbrakes trailer brake controllers that let an unauthenticated attacker within range apply or release brakes. Patches exist for EB2 and VM1; the older ELBC 2000 is still awaiting a fix.

- Affected products are the EB2, VM1 and ELBC 2000 brake controllers, used mainly in Australia and New Zealand according to CISA.
- Two critical flaws, missing authentication and weak replay protection, let an attacker within about 100 metres engage, release or adjust braking with no victim interaction.
- A third, medium-severity flaw in the firmware update mechanism could in theory allow persistent compromise; researchers did not demonstrate it.
- Firmware patches were released in early July for EB2 and VM1; a remediation plan for ELBC 2000 is

still being developed.

- No evidence of malicious exploitation has been reported.

Researchers at Element Digital, an Australian IT and cybersecurity consultancy, have disclosed three vulnerabilities in Bluetooth-enabled trailer brake controllers made by Elecbrakes. CISA published an advisory on the issues, noting the products are mainly used in Australia and New Zealand.

## What was found

The affected models are the EB2 (mounted on the trailer), the VM1 (mounted on the towing vehicle) and the older ELBC 2000. The controllers set the braking force applied to a trailer and can be operated through a dedicated remote or a smartphone app.

Two flaws are rated critical: missing authentication and insufficient protection against replay attacks. The researchers showed that an unauthenticated attacker within Bluetooth range, up to 100 metres, could use a laptop or phone to engage or release the brakes or change braking force, with no action by the victim. A third, medium-severity flaw concerns the firmware update mechanism. It could in theory allow persistent compromise, but the researchers did not attempt to install malicious firmware.

## Status of fixes

Elecbrakes was notified in mid-May and released patched firmware for EB2 and VM1 in early July. After patching, remote access requires an initial pairing that needs physical access to the device and cannot be done over Bluetooth. For the ELBC 2000, a remediation plan is still in development; the vendor advises owners to keep an active connection between the controller and their phone or remote while in use. The vendor told iTnews that about 40,000 app users were alerted and that the update reached 60-70% of controllers connecting daily. No malicious exploitation has been reported.

## Why it matters

The case shows how short-range wireless features in operational equipment can create physical safety risk when authentication is weak. Organisations that run vehicle fleets or equipment with similar components should confirm their exposure.

## What to do now

1. Check whether any trailers or fleet equipment use Elecbrakes EB2, VM1 or ELBC 2000 controllers, including those supplied through contractors.
2. Apply the vendor's firmware update to EB2 and VM1 units and record completion in the asset inventory.
3. For ELBC 2000 units, follow the vendor's interim guidance to keep the controller actively connected to its phone or remote during use, and track the pending remediation plan.

4. Include Bluetooth-enabled operational and vehicle equipment in asset inventories and risk assessments, covering authentication and update mechanisms.
5. Ask suppliers of connected equipment about their vulnerability disclosure and patching processes.