SALUS Controls PLC | Units 8-10, Northfield Business Park, Forge Way, Parkgate, Rotherham, S60 1SD, UK

# SALUS EV Chargers — Diagnostic Log Access Vulnerability

**Advisory ID:** ADVISORY-2026-0001
**SALUS Vulnerability ID:** VULN-2026-0001
**Status:** Published on 13 November 2026
**Severity:** Medium

## Summary

SALUS Controls PLC investigated a vulnerability in the shared FTP service used by certain SALUS EV chargers to upload diagnostic logs. Shared credentials embedded in charger firmware and insufficient access restrictions on the service allowed access to diagnostic logs associated with other chargers.

## Affected products

The following models have been identified as affected:

**EVT7UK, EVT7EU, EVT11EU, EV7UK, EV7EU, EV11EU, EV7FR and EV11FR.**

The reported issue was reproduced using EVT7UK firmware v2.2.3.

## Potential impact

The vulnerability could allow unauthorized access to diagnostic logs associated with other chargers using the shared FTP service. This access was demonstrated during the reported research investigation.

The affected FTP service has since been permanently disabled.

## Remediation and customer guidance

The affected FTP service has been permanently disabled. A firmware update addressing the vulnerability has been released globally.

If you own or manage one of the listed chargers and would like to confirm whether it has received the update, contact security@saluscontrols.com. Include your charger model and, if available, its installed firmware version. Please quote **ADVISORY-2026-0001**.

## Acknowledgment

SALUS Controls PLC thanks **Gareth Attrill** for reporting this vulnerability and cooperating with us during the investigation and remediation process.

## Further information

For information about reporting suspected security vulnerabilities, please consult the **SALUS Vulnerability Disclosure Policy** or contact **security@saluscontrols.com**.