ASSA ABLOY

SMARTair – Firebird Security alert for legacy versions (CVE-2025-54989)

As the global leader in access solutions, we take physical and digital security very seriously. We continuously work on strengthening the security for our customers and ourselves.

A zero-day vulnerability has been identified in all Firebird versions prior to:

- 3.0.13.33809
- 4.0.6.3203
- 5.0.3.1651
- and all 2.x previous versions

Once we became aware of the vulnerability, we immediately began assessing any potential impact on our products.

Since **TS1000** and **TESA Hotel tools** utilize Firebird, they may be affected.

However, **only installations with port 3050 open and accessible remotely** are potentially vulnerable. This scenario is **highly unlikely**, as both TS1000 and TESA Hotel software are designed for **on-premise installation**, with remote access typically handled via a web server.

What you should do:

- If you're running our software version 8.03.02 or higher → You're safe.
- If you're using an older version but port 3050 is NOT accessible → You're safe.
- If you're using an older version and port 3050 IS accessible → Action required:

1. Ensure port 3050 is restricted to trusted client connections only.
2. Plan an upgrade as soon as possible. Reach out to Smartair-st@tesa.es

Urtzi Zubiate
VP & Head of Spain & Morocco