NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-53984

Summary

CVE-2026-53984 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. Ground Station prior to 0.6.0 contains an unauthenticated database-destruction and arbitrary-data-injection vulnerability in the Socket.IO server's database_backup event handler that allows any unauthenticated network peer to wipe or replace the entire SQLite database by sending a single full_restore command with a caller-supplied SQL blob. Attackers can connect to the Socket.IO server on port 7000 without credentials due to disabled authentication enforcement and a wildcard CORS policy, then emit the database_backup event to drop every existing table and recreate the database from attacker-controlled CREATE TABLE and INSERT INTO statements executed via raw exec_driver_sql, permanently destroying all satellite records, orbital sources, hardware configurations, and observation schedules, or planting fabricated orbital-source URLs and observation entries that redirect the ground station to attacker-controlled servers on the next scheduled sync.

What we know

- **CVE:** CVE-2026-53984
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.