NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-70558

Summary

CVE-2026-70558 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. Dinky's POST /download/uploadFromRsByLocal handler passes the caller-supplied path parameter directly to new File(path) and file.transferTo(dest) with no path validation. The route is marked @SaIgnore and /download/** is excluded from the Sa-Token interceptor, so the only guard is a header equality check against a dinkyToken value whose default (efda1551-7958-4e0f-80a8-dfd107df3e38) is hardcoded in source and shipped to every deployment. Anyone who can reach Dinky's HTTP port (8888 by default) and supplies the hardcoded token can write arbitrary files as the Dinky service account. The default Docker image runs on 8888 with no proxy or authentication and chmod 777 on /opt/dinky, so the application's own classpath, launch scripts, and static assets are writable. Demonstrated impact: overwriting /opt/dinky/config/static/index.html served attacker JavaScript to admin browsers immediately, and writing /opt/dinky/org/dinky/Dinky.class executed attacker code as the Dinky service account at the next JVM start via a classpath-shadow launched by script/bin/auto.sh. Writes are uid 9999 (flink), not root, so /etc, /root, /home, and /usr are refused. Affects Dinky v1.2.5 (the current release) and the development branch, where the code is byte-identical.

What we know

- **CVE:** CVE-2026-70558
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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.