NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-69102

Summary

CVE-2026-69102 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. MaxKey contains an unauthorized access vulnerability due to a hard-coded JWT signing secret in application-maxkey.properties that allows unauthenticated attackers to forge valid JWT tokens and authenticate as any user by exploiting the password-skipped login endpoint. Attackers can craft a JWT token signed with the publicly known default secret, submit it to the /sign/login/jwt/trust endpoint, and obtain a fully authenticated admin session with access to SSO application configuration and downstream application secrets.

What we know

- **CVE:** CVE-2026-69102
- **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.