NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-67330

Summary

CVE-2026-67330 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. @better-auth/scim (a better-auth plugin) versions >= 1.4.0-beta.27 through <= 1.6.21 and >= 1.7.0-beta.0 through <= 1.7.0-beta.9 contain an authorization bypass. SCIM token issuance did not reject provider IDs already used by existing SSO, SAML, OIDC, generic OAuth, or social account providers, and the same logical provider ID was used for both SCIM provider configuration and account ownership. An authenticated user could mint a SCIM token whose provider ID collided with an existing provider namespace, causing SCIM user routes to resolve account rows the token never provisioned. This allowed listing, reading, updating (including rewriting global profile/email fields without uniqueness checks), and deleting global user accounts and sessions, resulting in account takeover and unauthorized deprovisioning. Fixed in 1.6.22 and 1.7.0-beta.10 (1.7.0-rc.0).

What we know

- **CVE:** CVE-2026-67330
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.9 Critical, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 0%

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, limit network exposure of the affected service and tighten access until patched. 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.