College Board confirms breach after unauthorized password changes



College Board says attackers used AI-assisted tools to find a flaw in its professional-account signup page, reaching registration and CSS Profile systems and triggering password resets. A linked breach at a third-party vendor is under investigation.

- Students reported unexpected password-change notices on Thanksgiving, all appearing to originate from the same location.
- College Board says attackers exploited a flaw in the signup page for professional accounts, found using AI-powered tools.
- Attackers could start password resets and view basic registration data such as names and email addresses.
- A third-party vendor that stores financial aid submissions had a separate, apparently linked breach;

> its scope is still being investigated.
>
> - New registrations and CSS Profile access are suspended, and the number of affected accounts has not been disclosed.

College Board, the nonprofit behind the SAT and AP exams and the CSS Profile financial aid service, has confirmed a data breach after students reported password changes they had not requested.

What happened

The organization says attackers reached the systems used to create new accounts and to submit CSS Profile applications. It told BleepingComputer that they used AI-powered tools to find a vulnerability in the signup page for professional accounts and then exploited it. This let them start password resets for some users and view basic registration details such as names and email addresses.

College Board says the issue affects a small portion of its users and that it is working with third-party experts on scope. Its repository of test scores and exam questions was reportedly not accessed. A third-party vendor that stores submitted financial aid information suffered a separate breach at the same time, believed to be linked, and the data involved is still being determined.

Response and impact

New account registration and CSS Profile access have been switched off temporarily, while existing users can still sign in. College Board plans further password resets for affected students, proctors and other professionals, and says more may follow. It has not said how many accounts are affected or when services will be restored. It is also working on ways to help families meet financial aid deadlines.

Why it matters

The case shows how a flaw in a low-profile registration page can lead to account takeover, and how a supplier holding sensitive submissions can widen exposure. Attackers reportedly used AI tooling to find the weakness, so organizations should assume such flaws may be found faster than before.

What to do now

1. Review the security of public registration, signup and password-reset flows, including rate limiting, verification and alerting on bulk resets.
2. Test externally facing portals for logic flaws, including less-used pages such as professional or partner account signup.
3. Confirm which third parties store your customers' sensitive submissions and ask for their incident-notification terms and security evidence.
4. Prepare a playbook for mass credential resets with customer notices and support coverage during

holidays and weekends.

5. If your institution handles personal data, check whether a similar incident would trigger notification duties under PDPL and sector rules such as the SAMA Cyber Security Framework.