Important Information from ZCS: PowerSchool Breach Archived

Rebecca Coffman • a year ago • Wednesday, Jan 8 at 4:02 PM • **Zionsville Community Schools**

Good afternoon ZCS Faculty, Staff, Parents & Guardians-

You may have seen in various news outlets today reports of a cybersecurity breach involving PowerSchool. Zionsville Community Schools is a client of PowerSchool, utilizing their various platforms and services for daily student and staff operations. I write today to share what we know about this incident as of this afternoon.

In the last 24 hours, PowerSchool clients have received messaging indicating a breach that their organization identified on December 28, 2024. The notification to ZCS indicated that this incident involved unauthorized access to certain information through one of the community-focused customer support portals, PowerSource. Their initial message to ZCS stated that "our thorough forensic investigation has confirmed that information related to other PowerSchool products you have were not affected as a result of this incident." PowerSource is a product that is not in use by ZCS students, parents, or teachers. The full letter ZCS received can be **viewed here.**

Upon discovery of the security breach, the ZCS Technology Department immediately began an internal investigation into all the district's PowerSchool-related products, and that investigation is ongoing. We have submitted a possible breach to authorities at the Indiana Office of Technology per state code. We are working with PowerSchool and security experts to determine if any exposure of ZCS data was included in their breach. If information has been exposed, we will begin to notify all affected individuals immediately.

This initial communication is to assure you that we are aware of the situation involving PowerSchool and will keep you updated as we monitor information and identify the steps needed to protect your information. As we learn more from our partners at PowerSchool, we will continue to update you.

Data privacy and security is a continual focus for our team. It is a responsibility we take seriously as an element of school safety. We are proud to be one of the few schools in the country to have received the Trusted Learning Environment seal through our continual efforts in this realm. More information about our ZCS Data Privacy and Protection plan can be **accessed here.**

We will continue to provide updates as we learn more. Thank you for your support of Zionsville Community Schools.

Sincerely,
Dr. Rebecca Coffman
ZCS Superintendent

Full letter shared below

Dear Valued Customer,

As a main point of contact for your school district, we are reaching out to make you aware that on December 28, 2024 PowerSchool became aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Your organization's

Technical Contact was informed of this incident earlier today. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool SIS customer data using a compromised credential.

However, our thorough forensic investigation has confirmed that information related to other PowerSchool products you have were not affected as a result of this incident. Please note there is no further action needed from you at this time relative to your non-PowerSchool SIS products, and we are simply notifying you to be as transparent as possible and because we value our partnership with you. We have already notified technical contacts responsible for PowerSchool SIS in your organization.

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.

We have also deactivated the compromised credential and restricted all access to the affected portal. Lastly, we have conducted a full password reset and further tightened password and access control for all PowerSource customer support portal accounts.

Importantly, the incident is contained, and we have no evidence of malware of continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience any operational disruption and continues to provide services as normal to our customers.

We are addressing the situation in an organized and thorough manner, following all of our incident response protocols. PowerSchool is committed to providing affected customers with the resources and support they may need as we work through this together.

Again, although your product was not impacted, we wanted to assure you that we are addressing the situation in an organized and thorough manner following all of our incident response protocols. Should you have any questions, please do not hesitate to contact your customer service manager. Thank you for your continued support and partnership.

Best,
Hardeep Gulati
Chief Executive Officer

Paul Brook
Chief Customer Officer

cc: **Mishka McCowan**
Chief Information Security Officer