Recent notes taken from PowerSchool webinar on 1/8/2025 communicating to school districts about the recent data breach.

CEO Hardeep Gulati

CEO greets. Provides cover and corporate speak. Acknowledges the responsibility they have, and that it should be contained. Assured they have taken every step possible. Confident that the breach is contained, understood, and no ongoing concerns on the system exist. Commitment to communication. We have assurances that the information is contained and will not be publicly available. And if there is PII released, monitoring should be in place. Powerschool takes security seriously, though this incident undermines it. They are increasing investment in security.

CISO Mishka McCowan

What happened

- Support contractor credentials were compromised. The name of the contractor is the one that appears in your logs.
- Powersource is a forum and remote support tool
- Powersource is used for remote support
- Attacker accessed maintenance credentials.
- The logs show clearly what was accessed and when.
- First instance: Dec 19.
- Dec 19-21, increasing activity while the attacker explored and prepared.
- Dec 22: The majority of exfiltration occurred
- The attacker downloaded the Student table, the teacher table, then move on to the next target.
- The speed and consistency of exfiltration indicates the attack was automated as of Dec 22.
- Dec 23: Activity reduced, was likely manual at this point. Most of it was done by then.

Timeline and PS Response

- Dec 28: Attacker notified them. PS engaged Crowdstrike.
- Identified the compromised account, which you see in your logs.
- Disabled the compromised account.
- Forced a reset of all PS credentials in that system
- Removed maintenance access from all accounts except four, which are incident response.
- Started to piece together what happened: What was downloaded (Student + Teacher).
    - Found no evidence of backdoor user creation
    - Found no evidence of other attack vectors via web
    - Found no evidence of other local software vulnerabilities
- Locked down Power Source

    - Put the employee portion behind VPN
    - Required password changes from employees
    - Disabled maintenance access on Hosted instances
    - On prem access remains at whatever you had it set to
- Moving forward PS will no longer have time-unlimited access. They will need to request access each time. Maintenance Access will not be turned by indefinitely. It will turn off automatically in 1-30 days and need new action to turn it back on later.
- Considering additional controls:
    - Breaking maintenance into its own application away from PowerSource
    - Looking into other ways to limit access from Maintenance to your SIS.
    - As PS rolls out more controls, they promise to be transparent so your SIS availability is not impacted by surprise.

Data impact

- Student and Teacher tables.
    - Student name, address, demo data, medical alerts, parent/guardian name, email, phone
- Crowdstrike report will be available late next week; perhaps slightly longer as they go through 15TB of logs.

Q&A

- MFA is enforced to log into the VPN where PowerSource is now accessed. Eventually MFA will be required for PowerSource support staff, too.
- Not sure if staff/students can be forced en masse to change passwords. Check with your Customer Support Manager.
- First indication of attack is Dec 19. Dec 22 is where most of the attack activity took place.
- There is no financial account information defined in the tables that were taken.
- CyberSteward negotiated with the attacker who provided video evidence that they were deleting the data. It shows the "shred" utility being used to delete the data. Provided assurances there were no copies prior to the shred.
    - How can we trust it? It is their business. Their reputation is part of that. However, Crowdstrike is going to continue monitoring Dark Web traffic to detect if they break their word.
- The student and teacher table should not contain password information. It used to, but it had been moved to another location and should say something like "MCAS MANAGED" instead of containing password data.
- On prem districts should turn off maintenance access. They will contact you to turn it back on if needed.
- PowerSchool says they will provide assistance with community communication.
- Most districts do not have PII in the Student Table. If your districts DOES have PII here, you will need to adjust your communication/notifications accordingly.
- PowerSchool will provide some high level statements to get things started, by the end of day today. Additionally they will provide communication plans as soon as possible (a few days)

working with you specifically, especially on on-prem customers, to determine what communication is needed.

- Credit monitoring for minors: Depending on your state regulations, and the PII in your table. We will work with you based on your impact to communicate directly and provide hotlines (??) Stay tuned for more info on this.
- When communicate, assure that the data is contained and will not be released. We will provide credit monitoring where warranted.
- PS is working to comply with each state's obligations and timelines. They promise to assist districts to comply. They are working to prepare a per-school analysis of the impact to support this notification.
- Customers with medical data may need to work with PS on HIPAA disclosures
- The compromised user may still appear to be connecting. However, this is just a bug. They have done a lot of testing to verify this is an mirage due to a bug.
- PS has a clear list of compromised schools, which was used to build notifications. If you got a notification, you were affected. Ask a CSM, providing your SIS URL, to check for sure.
    - If you don't know who your CSM is, send a support ticket. They'll reply promptly.
- Should we notify our Cybersecurity insurance? PS is building an FAQ. This is not yet available.
- Will PS be communicating with parents? They can provide it for Cloud easily. For On-Prem they need cooperation. If you want to communicate yourself, they'll provide a communication kit.
    - A high level statement will be sent to you soon, which you can use to get started
- Trends among targeted schools? No. The target was "Powerschool SIS", not any particular districts.
- To turn off maintenance access, reach out to your CSM for the documentation or help.
- There was no evidence that extensions or other data besides Student and Teacher tables was exfiltrated.
- Confirm: Maintenance access was disabled. On-prem customer need to do this themselves.
- Photos were not exfiltrated. The only photo-related data was a field that indicates whether a photo exists
- The total exfiltration is less than 1TB
- Canadian and US instances were compromised in the same way
- Some meaningless chatter about distinction about whether "schools" were attacked or PowerSource was attacked. . .
- Some more talk about how more answers are in FAQ, which will be updated.
- Notifications were sent about other products. It may have been too broad because of their haste. Oops.
- FAQ: Posted on Customer Community in the SIS section. Log in and visit this link
- As soon as PS can complete analysis, they will provide you with notification about YOUR data, and the disclosures and communication that YOU are required to make.
- No plug-in data was compromised. Student and Teacher table data only