Interim Fact Sheet

Background

On December 28, 2024, PowerSchool became aware of certain unauthorized activities by an unauthorized third party (the "Threat Actor") in their computing environment, specifically in their SIS database product.

This fact sheet provides factual background and data points regarding the Threat Actor's activities in the Company's IT environment based on forensic artifacts and logs.

Containment Status

On December 29, 2024, at 12:29:57 UTC, PowerSchool disabled the Active Directory (AD) account assigned to the user whose account was used in the unauthorized activity.

CrowdStrike Falcon, a leading 24/7 EDR monitoring and blocking software tool, was already deployed throughout the PowerSchool computing environment prior to the incident. Falcon Overwatch, a 24/7/365 threat hunting service was also already in place as part of PowerSchool's existing security program for threat detection support.

Key Factual Findings

The following is a summary of CrowdStrike's key factual findings and data points related to Threat Actor activity in the environment. This investigation is ongoing, and these findings are subject to change due to new evidence and analytical results.

1. **The Threat Actor leveraged the PowerSource access from the compromised user account in order to access PowerSchool's SIS platform.**

   On December 19, 2024, at 19:43:14 UTC, the Threat Actor performed their first access from PowerSource to SIS using the "Maintenance Access" functionality.

2. **CrowdStrike found no evidence of access or escalation of privilege by the Threat Actor to any PowerSchool systems beyond application-level access via the web-based interface.**

   CrowdStrike has found no evidence of system-layer access associated with this incident, nor any malware, virus, or backdoor.

3. **The last date of Threat Actor activity in the Customer environment occurred on December 28, 2024, at 06:31:18 UTC.**

   As noted above, PowerSchool learned of this incident on December 28, 2024. On that date, the Threat Actor used the compromised user credential to log in to the "Maintenance Access" interface of PowerSource to interact with the SIS database. CrowdStrike has observed no evidence of Threat Actor activity in the PowerSchool computing environment subsequent to December 28, 2024, at 06:31:18 UTC.

Appendix A: Indicators of Compromise

Table 1 provides a summary of the system- and network-based indicators of compromise (IOCs) that CrowdStrike identified in the environment.

Indicator	Indicator Type	Description
91.218.50[.]11	IP Address	This IP is associated with data exfiltration.
169.150.203[.]39	IP Address	This IP is associated with Threat Actor related PowerSource activity.
185.213.154[.]172	IP Address	This IP is associated with Threat Actor related PowerSource activity.
193.32.127[.]248	IP Address	This IP is associated with Threat Actor related PowerSource activity.
66.63.167[.]173	IP Address	This IP is associated with Threat Actor related PowerSource activity.

Table 1: Indicators of Compromise