CROWDSTRIKE SERVICES

CROWDSTRIKE

Investigation Report

PREPARED FOR

PowerSchool Group LLC

DELIVERED ON

February 28, 2025

services@crowdstrike.com

Table of Contents

Executive Summary

Background

On December 28, 2024, PowerSchool identified suspicious activity using credentials belonging to a support user ("compromised support credentials") in their PowerSchool Student Information System (SIS).[1] On December 29, 2024, CrowdStrike Services ("CrowdStrike") was engaged to provide investigative services and to assess the scope and extent of unauthorized third party ("Threat Actor") activity in the PowerSchool environment. CrowdStrike's investigation began on December 29, 2024, and concluded on February 17, 2025.

CrowdStrike is informed that following the security incident, PowerSchool took steps to prevent the data involved from further unauthorized access or misuse and to secure the impacted environment. CrowdStrike understands this involved:

- Deactivating the compromised credential
- Enforcing a full password reset for employees and contractors
- Restricting access to and tightening password and access controls for the affected customer support portal
- Requiring that access to the PowerSource environment be via company's VPN, which requires single sign-on (SSO) and multi-factor authentication (MFA)

In conducting the review, CrowdStrike observed that PowerSchool's endpoints and servers are protected by CrowdStrike's Falcon Endpoint Detection and Response (EDR) software, which provides advanced security monitoring, threat detection, next-generation antivirus, and real-time endpoint detection and response (EDR) capabilities. PowerSchool's systems are also protected by CrowdStrike's Falcon Overwatch, a 24/7/365 threat hunting service. In addition, CrowdStrike is informed that PowerSchool's systems and data storage was configured with AES-256 encryption for data at rest.

Objectives

CrowdStrike's objectives were to determine the following:

- How the Threat Actor gained access to the PowerSchool environment.
- The earliest and most recent dates of Threat Actor activity.
- Whether the Threat Actor moved laterally in the PowerSchool environment and, if so, how.
- Whether there was any evidence that the Threat Actor accessed or exfiltrated PowerSchool data and, if so, what data was accessed or exfiltrated.

[1] Per PowerSchool's website, PowerSchool SIS "provides back-office administrator functionality, as well as student-, parent- and faculty-facing functionality to manage key organizational information assets, including demographic data, enrollment, grades, transcripts, and other governmental agency reporting capabilities." See https://www.powerschool.com/operations/student-information-systems/.

- Whether the Threat Actor persists in the PowerSchool environment, or whether they have been evicted.

Scope

CrowdStrike's scope in the investigation involved performing the following:

- Review and monitoring of CrowdStrike Falcon ("Falcon") data.
- Review of Falcon Forensics Collector (FFC) data.
- Analysis of additional logs provided by PowerSchool.

Key Findings

The following is a summary of the key findings from CrowdStrike's analysis of available data.

1. **The earliest evidence of unauthorized activity attributable to the Threat Actor within the PowerSchool environment occurred on December 19, 2024, at 04:06:24 UTC.**

   At that time, the Threat Actor initiated an HTTP GET request for `support.powerschool[.]com` from IP address `146.70.128[.]186`.

2. **The Threat Actor performed Maintenance Remote Support operations in PowerSource to gain access to PowerSchool customers' SIS data.**

   Between December 19, 2024, at 19:43:14 UTC, and December 28, 2024, at 06:31:18 UTC, the Threat Actor performed Maintenance Remote Support operations in PowerSource, which enabled the Threat Actor to access the individual customer organizations' SIS instances. At 19:43:37 UTC, the Threat Actor initiated a Maintenance Remote Support connection to PowerSchool SIS from the same IP address using the compromised support credentials. Per PowerSchool's website, "PowerSource is a community-focused customer support portal for all PowerSchool products."[2] As such, PowerSource allows a support technician with sufficient permissions to gain access to customer SIS database instances for maintenance purposes.

3. **The Threat Actor exfiltrated data from the PowerSchool SIS instances of PowerSchool customers.**

   Between December 19, 2024, at 23:02:54 UTC, and December 23, 2024, at 08:04:45 UTC, the Threat Actor exfiltrated data from the `Teachers` and `Students` tables of the PowerSchool SIS instances for certain PowerSchool customers; CrowdStrike found no evidence of data exfiltration from any other tables.

4. **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 or malware associated with this incident. CrowdStrike also examined the tactics, techniques and procedures associated with the Threat Actor, as well as their actions taken in this incident, and did not identify any indications that PowerSchool customer IT environments outside of PowerSource and SIS were compromised or were at risk of intrusion due to this incident.

5. **CrowdStrike identified earlier evidence of unauthorized activity in the PowerSchool environment associated with the compromised support credentials between August 16, 2024 and September 17, 2024.**

   Beginning on August 16, 2024, at 01:27:29 UTC, PowerSource logs showed that an unknown actor successfully accessed the PowerSchool PowerSource portal using the compromised support credentials. CrowdStrike did not find sufficient evidence to attribute this activity to the Threat Actor responsible for the activity in December 2024. The available SIS log data did not go back far enough to show whether the August and September activity included unauthorized access to PowerSchool SIS data.

[2] https://support.powerschool.com/

6. **The most recent evidence of Threat Actor activity in the Customer environment occurred on December 28, 2024, at 06:31:18 UTC.**

   At that time, the Threat Actor used the compromised support credentials to log in to the maintenance interface of PowerSource to interact with PowerSchool SIS.

7. **CrowdStrike's dark web monitoring did not identify exfiltrated data for sale related to this incident.**

   PowerSchool engaged CrowdStrike's Recon+ Intelligence service as of January 2, 2025, to engage in dark web monitoring, and, as of the date of this report, CrowdStrike has not identified any evidence of information exfiltrated in this incident being made available for sale or download.

Investigative Methodology

CrowdStrike uses a combination of tools and investigative techniques to perform forensic and triage analysis of system and network data. This section provides an overview of those tools, techniques, and procedures followed in CrowdStrike's investigative methodology.

Falcon Forensics Collector (FFC)

FFC gathers artifacts from servers and workstations to support incident response triage, and compromise assessment analysis. This proprietary CrowdStrike tool implements data gathering modules and collects incident response-relevant data from the host. The tool places the data it collects into a database for CrowdStrike consultants to analyze en masse. FFC can collect numerous different types of system data to investigate present or historical threat actor activity. Data types collected by FFC include, but are not limited to, the following:

Microsoft Windows

- Disk Artifacts
    - Directory listing: A listing of targeted files from file paths on each host
    - File hashes: MD5 hashes of the files collected in the directory listing
    - Portable executable information: File metadata
    - Application Compatibility Cache: Execution tracked by legacy compatibility check
    - Prefetch and SuperFetch: Operating system (OS) optimization for frequently used files
    - Registry data: Forensically interesting keys and values from host registry hives
    - Event logs: Significant OS security, application, and system events
- Volatile System Information
    - Running processes: Processes that are currently running on the host
    - Shares: Mapped network folder shares
    - Network connections: Current network connections of the host
    - Domain Name System (DNS) cache: Volatile data on domain lookups stored for future use
- System Configuration
    - Scheduled tasks: Scheduled commands or batch scripts
    - Services: All services present on host
    - Users
    - Persistence locations

Linux/UNIX

- Disk Artifacts
    - Directory listing: A listing of all files from file paths on each host
    - File hashes: MD5 hashes of the files collected in the directory listing
    - Configuration data: Forensically interesting values from host configuration locations
    - Log data: Various logs in `/var/log` and `/var/adm`
- Volatile System Information
    - Running processes: Processes that are currently running on the host
    - Shares: Mapped network folder shares
    - Network connections: Current network connections of the host
- System Configuration
    - Cron Jobs: Scheduled commands or batch scripts
    - Persistence Locations
    - Services: All services present on host
    - Users

CrowdStrike Falcon

CrowdStrike Falcon is a suite of endpoint protection technologies that provide advanced security monitoring, threat detection, next-generation antivirus, and real-time endpoint detection and response (EDR) capabilities. Falcon continuously monitors and collects details of OS activity, such as process execution metadata, so that it can be analyzed for behavioral and threat intelligence-led indicators of attack.

During an Incident Response investigation, CrowdStrike uses this real-time telemetry to detect potential Threat Actor activity based on behavioral indicators of attack, indicators of compromise, and active threat hunting. CrowdStrike leveraged Falcon to triage potentially suspicious events and perform analysis on a system to determine if that behavior is malicious.

Log Analysis

CrowdStrike gathers or obtains access to relevant logs to support incident response investigations. Available log sources are identified, and the timeline of available data is documented. CrowdStrike consultants use a combination of tool-based analysis, en masse log searching, and manual event reviewing techniques to seek anomalous data in available log sources, indicative of attempts to attack a computer network or system.

CrowdStrike analyzed a variety of log sources, including but not limited to:

- Logs from network appliances:
    - Firewalls and Next Generation Firewalls (NGFWs)

        - Network connections
        - Network disconnections
        - Network traffic & NetFlow data
    - Web Application Firewalls
        - Connection data
        - HTTP access logs
    - Application Load Balancers
        - Connection data
        - HTTP access logs
- Web logs from Linux web servers
    - Access logs
    - Error logs
    - Catalina application logs
- Audit logging generated by the web applications that were the subject of unauthorized access

Microsoft Azure

CrowdStrike's Azure incident response methodology includes an assessment of available log sources, and subsequent, targeted collection and analysis of available logs for evidence of Threat Actor activity. Analysis is performed as per the MITRE ATT&CK taxonomy, with activity grouped into Threat Actor initial access, privilege escalation, lateral movement, and/or additional impact.

CrowdStrike's investigation also includes an evaluation of the Azure control plane configuration against a secure baseline, recognized by CrowdStrike as critical in defending against modern cloud security threats.

CrowdStrike may review any of the following key Azure components, where investigation-relevant log data is available, using a combination of automated and manual analysis techniques:

- Azure Infrastructure as a Service (IaaS) and Active Directory Logging
    - Azure Active Directory (AD) Interactive Sign-in logs
    - Azure AD Non-Interactive Sign-in logs
    - Azure Service Principal Sign-in logs
    - Azure Managed Identity Sign-in logs
    - Azure AD Audit logs
    - Azure Subscription Activity logs
    - Azure Service Bus logs
    - Azure API Management logs
    - Azure Load Balancing type service logs

    - Azure Network Security Group Flow logs
    - Azure Storage Account logs
- Identity and Access Management and Encryption
    - Azure Active Directory
    - Azure Key Vault
- Security Monitoring and Alerting
    - Azure Security Center
    - Azure Identity Protection

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 from PowerSchool SIS in December 2024.
146.70.128[.]165	IP Address	This IP is associated with data exfiltration from PowerSchool SIS in December 2024.
96.44.191[.]140	IP Address	This IP is associated with data exfiltration from PowerSchool SIS in December 2024.
169.150.203[.]39	IP Address	This IP is associated with PowerSource activity in December 2024.
185.213.154[.]172	IP Address	This IP is associated with PowerSource activity in December 2024.
193.32.127[.]248	IP Address	This IP is associated with PowerSource activity in December 2024.
66.63.167[.]173	IP Address	This IP is associated with PowerSource activity in December 2024.
146.70.128[.]186	IP Address	This IP is associated with PowerSchool SIS activity in December 2024.
193.32.162[.]96	IP Address	This IP is associated with PowerSchool SIS activity in December 2024.
146.70.174[.]52	IP Address	This IP is associated with PowerSchool SIS activity in December 2024.

Table 1: Indicators of Compromise