Incident Response Report: Premium House Lights Inc.

Curtis Crawford

Lighthouse Labs

2024

Contents

[Executive Summary 2](#_Toc180586697)

[Incident Timeline 2](#_Toc180586698)

[Technical Analysis 3](#_Toc180586699)

[Attack Origin and Impact 3](#_Toc180586700)

[How Systems Were Accessed 3](#_Toc180586701)

[Weaknesses That Allowed the Incident to Occur 3](#_Toc180586702)

[Incident Response 4](#_Toc180586703)

[Steps Taken to Contain and Remediate the Incident 4](#_Toc180586704)

[**Post-Incident Recommendations** 4](#_Toc180586705)

[Future Protection Against Similar Attacks 4](#_Toc180586706)

[Security Policy Adjustments 5](#_Toc180586707)

[Appendix 5](#_Toc180586708)

[Premium House Lights Network Diagram 6](#_Toc180586709)

## Executive Summary

Premium House Lights Inc. experienced a data breach that compromised customer data stored in the phl database. The attacker gained access to the company’s webserver, elevated privileges to root, and then proceeded to exfiltrate customer data from the database. This report outlines the key findings from the investigation, a timeline of the incident, technical analysis, and recommendations for remediation and future prevention.

## Incident Timeline

* **19/Feb/2022 21:56:11**: Suspicious activity began with HTTP requests from two IPs, **136.243.111.17** and **138.201.202.232**, through a bot, possibly probing the site for vulnerabilities. This activity was logged but appeared non-threatening ​(phl\_access\_log (1))​(phl\_access\_log).
* **19/Feb/2022 21:58:22**: Probing escalated when IP **138.68.92.163** began sending numerous 404 HTTP requests, attempting to access non-existent resources like /randomfile1, /archive, /software, and others. These actions suggest the attacker was testing for vulnerable endpoints ​(phl\_access\_log (1))​(phl\_access\_log).
* **19/Feb/2022 22:00:27**: Netstat command executed on the webserver, likely used to examine open ports and active network connections​ (phl\_database\_shell).
* **19/Feb/2022 22:00:55**: The attacker connected to the MySQL database as root via a socket. They proceeded to query for database information ​(phl\_database\_access\_log).
* **19/Feb/2022 22:01:45**: The attacker created a database dump of the phl database using the mysqldump command ​(phl\_database\_shell).
* **19/Feb/2022 22:02:26**: The phl.db file was exfiltrated to a remote server with the IP **178.62.228.28** using SCP (secure copy) ​(phl\_database\_shell).

## Technical Analysis

### Attack Origin and Impact

The attack originated from suspicious activity involving IPs probing the webserver, which culminated in unauthorized access. The attacker managed to escalate privileges on the webserver and gained root access to the MySQL database. Customer information from the phl database was extracted and transferred to a remote server.

* **Evidence**: The database access logs show SQL queries executed by an unauthorized user, and the shell logs reveal that the attacker performed a dump and exfiltration of the customer database ​(phl\_database\_shell)​(phl\_database\_access\_log).
* **Exfiltration**: The file phl.db containing customer data was transferred to an external IP, **178.62.228.28**, which marks the data exfiltration phase ​(phl\_database\_shell).

### How Systems Were Accessed

The attacker exploited vulnerabilities on the webserver, possibly due to weak configurations, which allowed privilege escalation to root. Once they had root access, the attacker connected to the MySQL database using a socket connection with root credentials, queried the customer database, and then exported it ​(phl\_database\_access\_log)​(phl\_database\_shell).

### Weaknesses That Allowed the Incident to Occur

* **Lack of network segmentation**: Both the webserver and the database were on the same VLAN without adequate network isolation. This allowed the attacker to pivot from the webserver to the database once initial access was obtained ​(phl\_database\_shell).
* **Weak privilege controls**: The attacker successfully escalated privileges to root on the webserver, indicating potential weaknesses in access controls or misconfigurations ​(phl\_database\_shell).
* **Insufficient database security**: The MySQL database was accessed using root credentials. There were no measures in place to restrict this type of access to specific hosts, allowing the attacker to connect from the compromised webserver ​(phl\_database\_access\_log)​(phl\_database\_shell).

## Incident Response

### Steps Taken to Contain and Remediate the Incident

1. **Isolate the affected systems**: The compromised webserver and database were immediately isolated from the network to prevent further data exfiltration and unauthorized access.
2. **Credential rotation**: All administrative and root credentials for the webserver and database were rotated. Multi-factor authentication (MFA) has been mandated for all administrative accounts.
3. **Block malicious IPs**: IP addresses associated with the attack (e.g., **178.62.228.28**) were blocked at the firewall level to prevent future access from those sources ​(phl\_database\_shell).
4. **Forensic analysis**: A full forensic analysis of the affected systems was conducted to understand the scope of the attack and ensure that no additional backdoors or malware were left behind.
5. **Review of system logs**: The webserver, database, and network logs were reviewed to confirm the full extent of the breach and identify additional suspicious activity ​(phl\_access\_log (1))​(phl\_access\_log).

## **Post-Incident Recommendations**

### Future Protection Against Similar Attacks

1. **Network Segmentation**: Implement network segmentation by placing the database in its own secure VLAN, separate from the webserver and other resources. This will limit the attacker's ability to pivot between systems ​(phl\_database\_shell).
2. **Privilege Management and Hardening**: Implement role-based access control (RBAC) with the principle of least privilege. Ensure that no services or users can escalate to root without multi-layered approval and review mechanisms ​(phl\_database\_shell).
3. **Database Security Enhancements**:
   * Enforce **host-based restrictions** on MySQL access to ensure that only specific, trusted hosts can connect to the database.
   * Use encryption for database backups and data in transit.
   * Implement **SQL monitoring tools** to detect suspicious queries and rate-limiting on sensitive operations (e.g., data exports).
4. **Regular Vulnerability Assessments and Patch Management**:
   * Perform regular vulnerability scans and patch management processes, especially on publicly exposed services like the webserver, to mitigate the risk of common exploits ​(phl\_database\_shell).
   * Conduct penetration testing to identify weaknesses in the system and correct them before attackers can exploit them.
5. **Incident Response Training and Testing**:
   * Develop and regularly update an incident response plan that includes specific steps for isolating and investigating compromised systems.
   * Regularly train staff on incident response protocols and simulate attack scenarios to improve response times and actions.

### Security Policy Adjustments

1. **Logging and Monitoring**:
   * Enhance logging capabilities across all critical systems to capture more detailed activity data, particularly for database access and administrative commands.
   * Set up a centralized logging server that aggregates logs from all systems and uses alerting mechanisms to notify the security team when suspicious activity is detected.
2. **Enforce Strong Password and Authentication Policies**:
   * Require all users, especially those with administrative privileges, to use strong, complex passwords and rotate them regularly.
   * Enforce multi-factor authentication (MFA) for all administrative users across all services, including the database.

## Appendix

* **Network Diagram**: (Attached)
* **Log Files**: Webserver access logs showing malicious activity​ (phl\_access\_log (1))​(phl\_access\_log). Database access logs revealing unauthorized queries ​(phl\_database\_access\_log).
* Shell history logs indicating the exfiltration of the database (phl\_database\_shell).

## Premium House Lights Network Diagram