Light Security: Discovering Vulnerabilities in Theatrical Lighting Control Systems and Assessing Their Prevalence

Brian K. Douglas, Jr.
Colgate University
bdouglas@colgate.edu

Aaron Gember-Jacobson
Colgate University
agemberjacobson@colgate.edu

Abstract

Theaters, concert halls, and other entertainment venues rely extensively on networked lighting control systems. These systems have been developed with a focus on convenience and creative flexibility, so they often lack standard security features. This poster characterizes the multiplicity of vulnerabilities based on experiments in theaters at two educational institutions and a survey of hundreds of lighting professionals across diverse venues. We find that 72% of surveyed venues are vulnerable, with the risk rising to 98% in large venues.

1 Introduction

Modern live entertainment venues, such as theaters and concert halls, rely extensively on networked lighting control systems to deliver dynamic performances. These systems allow for remote operation, real-time cue execution, and flexible integration across multiple components—including consoles [9], show-control software [12], DMX nodes [17], and light fixtures—using Ethernet, Wi-Fi, and multiple entertainment technology protocols [1, 2, 18] (Figure 1).

These systems were developed with a focus on convenience and creative flexibility, so they often lack standard security features like authentication and access control. Many lighting system components can be accessed and controlled from any device on the local private network. Connecting to the network can be trivial, because all network jacks in a venue are typically enabled (to permit flexible lighting placement), and many networks incorporate WiFi access (to allow lights to be managed from mobile devices). Furthermore, publicly

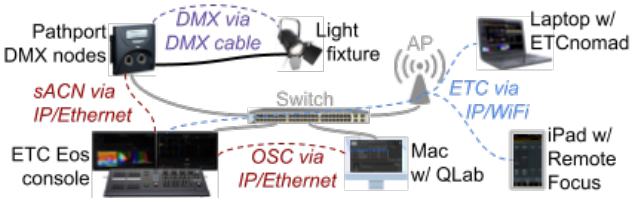

Figure 1: Architecture of a Lighting Control System

available control software automatically discovers and provides controls for consoles and DMX nodes on the same subnet [5] without authentication. Manufacturers that incorporate authentication mechanisms readily provide instructions to disable these features [16], and practitioner guides focus on reliability and interoperability rather than security [11].

Despite the potential for significant operational and financial harm, the prevalence and severity of vulnerabilities in live entertainment lighting control systems has not been widely studied. To address this gap, this poster presents an initial investigation into the security of these systems. Through a combination of hands-on experimentation in theaters at two educational institutions and a survey of hundreds of lighting professionals across diverse venues, we assess the real-world exposure of these systems to cyber threats. Our findings reveal that 72% of surveyed facilities are vulnerable to attacks, with the risk rising to 98% in large venues with a capacity of 600+.

2 Vulnerabilities Identified

To identify vulnerabilities, we conducted controlled experiments with a professionally installed lighting system in Colgate University's new Experimental Exhibition and Performance Lab. The system (Figure 1) includes: an ETC Ion XE console [9]; Pathport DMX-Ethernet gateways [17], which use Streaming Architecture for Control Networks (sACN) [1] to communicate with the console and Digital Multiplexing (DMX) [2] to communicate with light fixtures; a Mac running QLab [12], which communicates with the console using Open Sound Control (OSC) [18], and ETCnomad [5], which can

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

mirror the console; an iPad running ETC's remote control software; an Aruba wireless access point and switches; and many wall plates with network jacks.

The vulnerabilities fall into two broad categories: *console-level* and *node-level*. All attacks presuppose network access (wired or wireless) and placement in the correct subnet. We found this to be trivial given active wall jacks throughout the space and the presence of multicast sACN traffic in packet captures whenever the console is on (lights may be off).

Console-Level Attacks: With access to the lighting network and an IP address in the correct subnet, an attacker can connect to the ETC console via publicly available remote-control software [5]. The attacker need not know the IP address of the console, because the software automatically discovers it. From this software, an attacker can control light fixtures, exfiltrate programmed show data, change cues, or perform any other function that can be done from the console itself. ETC Eos does not support passwords for connecting.

An attacker can also send commands directly to the console using tools such as Send OSC [15]. Determining the console's IP address is trivial using standard scanning tools [14]. While OSC commands can control specific channels, cues, etc., the attacker need not know any of these to issue generic commands such as `/cs/playback/go` to run the next cue or `/cs/playback/gotocue/out` to turn off all light fixtures [7].

Node-Level Attacks: Attackers can connect to DMX nodes using manufacturer-provided control software [6, 17], and either modify configuration settings or manipulate individual light fixtures. To do this, one must know the IP addresses of the nodes, which is easily determined by using tools such as arp-scan [14]. Some nodes support password protection [17], but this doesn't prevent flooding or spoofing of higher-priority multicast sACN messages, resulting in node freezes or denial of service for legitimate control data [3, 4, 10].

Consoles and nodes also often support standard modes of remote access (e.g., telnet, SSH) and either do not require authentication or ship with default credentials. Direct access to these devices permits configuration changes, or even arbitrary code execution, that persist across performances.

3 Prevalence of Vulnerabilities

To study the prevalence of the aforementioned vulnerabilities, we attempted these attacks at another venue (with permission), and we distributed an anonymous survey (IRB approved) through active lighting/theater technician Facebook groups.

Field Study: We attempted a subset of the above attacks at a mid-sized theater at a small college. We connected to network jacks readily available and accessible from audience areas, identified the appropriate subnet through packet captures, and discovered devices using nmap. Our attempts to remotely connect to and send OSC messages to the ETC Ion XE console were initially unsuccessful because the console was shutdown. However, once the console was powered on (as it would be during a show) we could control all of the ETC Smartbar nodes, and connected lighting fixtures, by mirroring the console. Even with the console powered-off, we could still control all nodes using our own virtual console, injected sACN messages, or a direct telent connection. None of these methods of control required authentication.

Our scans also uncovered an ETC Paradigm control system for theater house lights [8], which did not exist in the system at Colgate. No authentication was required to access the web interface and disable wall switches, alter lighting levels, delete configurations, or disable the system entirely. We also observed that a malformed web request could make the system non-responsive and require a hard restart.

Industry Survey: To study the prevalence of vulnerabilities across many venues, we advertised an anonymous survey on six lighting design Facebook groups (totaling 388K members) and the QLab Google Group. The survey asked respondents about their venue's lighting hardware, network configuration, and general characteristics such as seating capacity. We received 333 responses from lighting professionals across university, public, touring, and commercial venues, with 45% of venues having a seating capacity ≥ 600.

Across all respondents, 65% reported enabling WiFi access for control networks, and 62.5% used secondary control devices (mobile or desktop). Of these, 40% used mobile remote-control software and 39% used desktop applications to interact with their lighting consoles. Protocol adoption varied among those who responded to the respective question: 85.9% of venues incorporated OSC for show control messaging, while 70% employed sACN for DMX-over-IP transport.

Overall vulnerability analysis indicates that 72% of facilities were susceptible to at least one network-based attack vector. This risk escalates with venue size: among venues with seating capacities of ≥ 600, 98% were vulnerable, compared to 72% in smaller venues.

4 Conclusion & Future Work

Our findings demonstrate that widespread use of unsegmented networks, publicly available control software, and unsecured protocols contributes to substantial security gaps in live entertainment lighting control systems. Our planned future work includes: (1) conducting additional site visits to further validate our findings and uncover new vulnerabilities; (2) extending our study to audio and video control systems, which similarly have limited/no authentication and unencrypted control channels; (3) evaluating the technical feasibility and usability of common network security measures, such as segmenting using VLANs, TLS-encapsulating OSC/sACN, hardening device configurations, and monitoring for traffic anomalies; and (4) developing targeted educational programs to raise security awareness among lighting and production professionals through organizations like the United States Institute for Theatre Technology (USITT) [13].

References

[1] Entertainment technology - Lightweight streaming protocol for transport of DMX512 using ACN. ANSI E1.31 - 2018, American National Standards Institute, 2018.

[2] Entertainment technology - USITT DMX512-A asynchronous serial digital data transmission standard for controlling lighting equipment and accessories. ANSI E1.11 - 2024, American National Standards Institute, 2024.

[3] Antirez. hping3. https://www.kali.org/tools/hping3/.

[4] Philippe Biondi and the Scapy Community. Scapy. https://scapy.net/.

[5] Electronic Theatre Controls. ETCnomad. https://etcconnect.com/ETCnomad/.

[6] Electronic Theater Controls. Concert Software. https://www.etcconnect.com/Products/Networking/System-Configuration/Software/Concert.aspx.

[7] Electronic Theater Controls. OSC Commands. https://www.etcconnect.com/webdocs/Controls/ColorSourceAV_onlinehelp/en/Content/CommandsOSC.html.

[8] Electronic Theater Controls. Paradigm Systems. https://www.etcconnect.com/Products/Architectural-Systems/Paradigm/.

[9] Electronic Theatre Controls. Eos family consoles. https://etcconnect.com/Products/Consoles/Eos-Consoles/.

[10] Electronic Theatre Controls. Difference between sACN per-address and per-port priority. https://support.etcconnect.com/ETC/Networking/General/Difference_between_sACN_per-address_and_per-port_priority, June 2022.

[11] Electronic Theatre Controls. Network Design. https://support.etcconnect.com/ETC/Networking/General/Network_Design, February 2024.

[12] Figure 53. QLab. https://qlab.app/.

[13] United States Institute for Theatre Technology (USITT). Education & training. https://usitt.org/usitt-education-training.

[14] Roy Hills. arp-scan. https://www.kali.org/tools/arp-scan/.

[15] Dominic Sacre. Ubuntu Manpage: send_osc - Sends a single OSC message. https://manpages.ubuntu.com/manpages/xenial/man1/send_osc.1.html.

[16] Pathway Connectivity Solutions. Entertaintment network security. https://pathway.acuitybrands.com/resources/network-security.

[17] Pathway Connectivity Solutions. Pathport DMX gateways. https://pathway.acuitybrands.com/products/family/pathport-dmx-ethernet-gateways.

[18] Matthew Wright, Adrian Freed, and Ali Momeni. Opensound control: State of the art 2003. In *Proceedings of the International Conference on New Interfaces for Musical Expression*, pages 153–159, 2003.