Pwning a $60,000 Lighting Console in a Few Minutes

Posted Aug 19, 2022 • Updated Aug 21, 2022

By Parzival

17 min read

Act 1: Opening

A significant amount of time and effort go into preparing the sound and lighting for a concert. Having once been in charge of both for theatre productions, I know just how stressful it can be when a microphone stops working mid performance or when the timing is a few seconds off on a lighting cue.

Something that I always wished for when working in theatre tech was the ability to tweak the lighting and sound remotely. Often times I had to hop down from the control booth, check on something, and quickly climb back up my ladder. It would have been significantly easier to tune settings from either my phone or laptop on the fly.

Well, apparently that's possible now and I'm just getting old. Controlling a lighting console either via a mobile application or remote control appears to be common now - especially since we can just connect the console to WiFi *because connecting everything to WiFi is a good idea*.

Thus begins the story of how I obtained a root shell on a $60,000 lighting console in a few minutes. Keep in mind that this did not require some fancy exploit or l33t out of the box thinking - **spoiler** all it took was connecting to an unsecured access point, a quick ping sweep, port scan, and trying some 'dumb' default credentials on a remote service.

Act 2: The First Mistake

Everything started one Thursday night when I attended a metal show. If you know anything about me, it's that I **love** doomscrolling on Twitter. Arriving to a metal show about an hour early and learning that there was no cellular connection in the venue meant that reading InfoSec drama on Twitter wasn't a possibility and my suffering was imminent.

So what does everyone do when they have no cellular connection? We look for open access points; bonus points if those access points don't have a captive portal (looking at you Starbucks and Barnes & Noble).

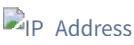
Sure enough, upon popping open the trusty hacker tool "Settings" on my iPhone and carefully navigating to the "WiFi" menu, I identified an open access point named "WAVLINK-N".

Now, before we even start scanning. Let's run a quick Google search for "WAVLINK-N" to see what comes up. One of the first results is how to sign into a WAVLINK network device, allowing us to easily enumerate that we've connected to a WAVLINK router:

If you've gone anywhere and asked for the WiFi password before, then you know that they will (mostly) always hand you access to the guest network - meaning that you are unable to access back of house devices such as the security cameras, PoS systems, music streaming system, or anything else that the business has hooked up.

Note: This is not always the case. The coffee shop I frequent asked me to perform some light scanning of their network to see if "anything came up". Upon scanning I observed that their recent security camera installations were connected to the guest network - a misconfiguration which allowed me to watch myself drink a caramel macchiato (so cool).

This is what I expected to be the case until I observed I was placed onto the 192.168.10.0/24 subnet. Big oops.



This means that we can access the Router login accessible at http://192.168.10.1 as stated in the previously identified documentation. If we wanted to launch exploits at this router we could attempt to search for WAVLINK router vulnerabilities, login with default credentials, and/or brute force valid credentials to the login.

Well, out of pure curiosity I attempted to sign-in with default credentials using the password `admin` but was unsuccessful. That's fine but now I'm getting *very* curious, let's run a ping sweep to see if we can identify any other devices.

> Quick note, I am friends with one of the managers of this venue so please don't cancel me for doing hard crime. I verified prior to scanning that I was clear to poke around a little bit (and not break anything).

Act 3: The Scanning

Let's address something really quickly before going any further. I'm an iPhone user.. I know, laugh it up. But that means my methods of scanning a network when I don't have my laptop are limited. Personally, I like using Fing for quick scans. It's also worth mentioning that there are several benefits to the app if you're not a l33t hax0r such as scanning an Airbnb rentals network to identify hidden cameras (but that's a topic for another day, I'm not sponsored). `/rant`

This is also to preface that I wasn't able to take too many screenshots of this device, and they're all off of my phone. I was too busy headbanging and hanging out with good people to remember that I should screenshot everything I was observing at the time. Additionally, the following day when notifying my PoC they wanted to immediately fix this console and remove the access point (I might get some time around the holidays to mess around with this console further though).

Anyways, back on topic. When I see ftp and/or ssh enabled, I want to try seeing if I can authenticate to the `root` user with default or weak credentials. Do you see where I'm going with this? Keep in mind, at this point in time I had no information or what device this actually was. The following screenshot demonstrates that I was able to use Termius to attempt to SSH into the device:

I know.. Not the greatest screenshot. It would be signifcantly more satisfying if I had CrackMapExec or Hydra installed on my phone to have the "password found" displayed.. Nevertheless, I attempted to login with the password `toor` originally which was unsuccessful.

Following this, I tried the most complex password I could think of and attempted to sign-in with the password `root` .. Surely enough, I soon observed that I successfully was dropped into a shell on the system:

Oh boy.. fourteen minutes before the show starts and I have obtained a shell on something called `grandMA2-light` . Chills. Prior to running any commands, the first thing I am going to do is run a quick search for the hostname and see what comes up:

Things are starting to quickly make sense. It looks as though the console can actually do more than lights, there's also the possibility of controlling "video and media" as stated in the description. Next I want to actually see what the device looks like, which did not disappoint:

Damn.. This looks awesome, it can probably run DOOM. From reading some of the documentation I also learned that you have access to the command line on the device. Taking an image from the documentation, it should look a little like this:

Upon a little more research, I came across the price of this unit (originally), this is when I decided on the name of this post:

Yep. You are reading that correctly. Having seen this beast in person, I believe it it is the `grandMA2 light` version (as referenced in the hostname). It is probably the most expensive shell I've ever popped.

So what next? Well, I ran a few commands on the system. Sadly I didn't screenshot them all but I did find some interesting things in the short period of time I had. I first enumerated binaries on the host and observed that I was dropped into your standard `bash` shell. Additionally, binaries that would be installed on a typical Linux system were available to me.

After confirming that I would be able to run commands and I wasn't in some type of limited environment, I decided to run `ifconfig` to display some basic information about the configured interfaces:

That's always some good information to have. I was also interested in running `netstat -ant` to view network connections for the device:

We see some interesting information here such as a HTTP service, and other TCP ports such as 80, 6000, 7001, 7003, 7005, 30000, and 30001 which are listening. While I would love to investigate all of these, I sadly did not have the time. If I had to guess, these are most likely used by the device for different features such as lights, LEDs, and video.. It's hard to guess since there's so much going on under the hood.

One of the more interesting things I found was from running `ps -aef` on the device:

It always feels like a CTF when I see a custom binary. I observed two interesting files here, namely `/usr/sbin/gmad` and `/data/ma/actual/gma2` . With the concert being so close to starting, I was hesitant to mess with either of these "in prod". I can only imagine that removing the `gmad` binary would be devastating and require the system to be reset in some capacity.

Otherwise, I wasn't able to find anything else of interest within time I had on the device. As I mention later on in this article, it was revealed that the device runs a "Custom Linux OS". From my observations this looks as though it's just an Ubuntu installation with some custom binaries and minor configurations made. There doesn't appear to be any hardening done on the system that I observed, it's likely that uploading your tool of choice (such as Nmap or Responder) would function perfectly fine if you installed the appropriate dependencies.

Act 4: Contacting the Vendor

Following the concert, I decided to reach out to the vendor, 'MA Lighting' and request information on my findings. When asking my point of contact, they stated that it was unclear if someone had manually made those changes as it was an older lighting console. In my first email I asked the following:

> Good afternoon,
>
> I recently performed a small network audit and identified a grandMA2 lighting console. I was able to successfully SSH into the device to obtain root-level access with the credentials: root:root.
>
> Is this the default configuration for the device? Is changing the root accounts password acceptable or will this cause issues with the console?

The reason I ask if changing the credentials on the device would cause any issues is simply because this is a device I hadn't even heard about until last night. I was unsure if there was some SSH magic going on under the hood, and/or if the credentials were required some other functionality I wasn't unable to identify.

A few days later I received a reply from MA Lighting stating that changing the SSH credentials stating the following:

> Yes, you can change the SSH credentials if you would like - it should not affect the performance of the desk. The updated credentials will persist through software updates as well, unless you have to perform a Factory Reset.

Perfect! We now know how to remediate the identified issue. I forwarded this information to my contact and sent another email to MA Lighting asking again if the identified credentials of `root:root` were the default for the device. I was told the dev team would need to answer that and they'd be in touch. Surely enough, after waiting a few days I received a reply stating the following:

> Yes, SSH is enabled by default, and those are the default credentials. However, because the consoles are a custom Linux OS with no personal, medical, or financial data stored on them, the devs haven't felt the need to change this.

Well, that's half the answer I was expecting. While I understand the reasoning, it's now my job to state the risks of this system having default credentials. I sent a reply with the following information shortly after (I redacted a few sentences with links provided at the bottom of this post):

> Alongside the risks I detailed in the previous email such as the lighting console being used as a foothold on the network, and DoS attacks being conducted against it - default credentials with a remote management port exposed by default as SSH being open is a high-risk issue that would allow for an attacker to potentially establish persistence, and attack other devices on the network.
>
> If SSH is not required (which it does not appear to be, from my understanding), it should be disabled. Alternatively, users could be provided with a randomly generated password upon setting up the device.
>
> There are multiple CVE's associated with default credentials. I plan to request one to be used for reference on this issue. I'd love to assist in the process and align with your internal standards of this. Please let me know if this issue is something that the dev team will fix or release guidance on in the near future!

I received a reply the following week which I do not want to completely share the details of since I think they *could* be considered sensitive so I'm going to hit you with a brief summary, broken down into a few points in the following section.

The Breakdown

MA Lighting stated that the grandMA2 was designed for isolated networks, not public networks. While to no fault of their own, customers who are not aware of the risks will place it in the first place it works.

Additionally, MA Lighting stated that changing the grandMA2 so that SSH and Telnet access work differently be default would require serious work on the operating system. At this stage of the grandMA2's development, this is unlikely to happen.

grandMA3 (the successor to grandMA2) is designed with being a part of public networks. There is no longer Telnet access to Linux and additional access can be disabled within the Mode2 software. Additionally, SSH is enabled but no longer uses the default credentials.

Act 5: The Finale

To be honest, I thought the reply from MA Lighting was more than sufficient. While the grandMA2 appears to have multiple security issues, it's appears as though these have been remediated with the release of the grandMA3.

If the message wasn't clear, this is *very* bad regardless of how common this device is. With little effort, I was able to obtain a root shell, and established a very good foothold on the network. Additionally, it's extremely likely I would be able to easily upload and/or download whatever binaries I wanted to the system.

There's also other considerations to take into account. For example, as stated in my emails to MA Lighting I could have ran a DoS attack against the system such as a 'Fork bomb', it's possible that the system would be rendered completely inoperable. Alternatively, an attacker could reboot, shutdown, and/or delete inportant binaries on the system.

While I'd love to believe that rebooting the device would turn off all the lights in the venue like something from Watchdogs.. From my extremely brief background in theatre tech, it is more likely that it would render the lighting console inoperable until it has successfully rebooted, the lights would most likely freeze in their current "cue". The tech would then be able to move forward to the next "cue" once the system rebooted and resume the show without a blackout. There'a also the possibility that an attacker would be able to connect to the device with the appropriate MA Lighting software and take remote control of the system, sabotaging the show in the process.

Although this system is unlikely to be encountered in your 'typical corporate environment', they exist out there. Personally, an opportunity has never presented itself to me where I can mess around with tech equipment such as a sound and/or lighting console but it's an area of devices that seems to have gone completely under the radar.

Additionally, something worth mentioning about this issue is that the target audience for this device is most likely not aware that SSH is open in the first place. I could not find documentation online discussing the use of the default credentials, nor any information about the 'Custom Linux OS'. It's likely if you find one of these in the wild, it's going to have SSH wide open.

Finally, (I promise, final thought) I haven't seen any security research of these devices before. I would not be surprised to discover that similar devices are using default credentials or are vulnerable to other low-hanging fruit vulnerabilities. This is an area of security that seems to be unexplored and I'm looking forward to hopefully raising some awareness.

I'll happily pentest your lighting/sound consoles for some coffee :)

Timeline

- April 7 - I attend a metal show, have no WiFi, connected to an open access point, and burgled a root shell on a lighting console more expensive than my college debt.
- April 8 - I notified the PoC I have at the venue of the finding and messaged MA Lighting asking for clarification on the devices default configuration.
- April 14 - Heard back from MA Lighting and began to discuss the default configuration of the device and how to remediate this issue.
- April 16 - MA Lighting replied and stated that they would need to get information from their developers to determine if both SSH was open, and the credentials `root:root` were used by default.
- April 20 - MA Lighting informed me that these were the default credentials, SSH is open by default, and the developers of the grandMA2 did not see this as a security risk. The reasoning provided was that the system doesn't store any financial/personal data. I replied to the email detailing what the host could be used for, possible system disruption, and providing appropriate references to CWE and MITRE ATT&CK.
- April 26 - Received reply from MA Lighting with additional information, stating that the issue is unlikely to be resolved and the following release (grandMA3) has remediated the issue identified.
- April 26 - Requested a CVE from MITRE.
- August 20 - Sent a follow up email to MITRE, published this blog post and was assigned CVE-2022-30036.

FAQ

Were you able to doomscroll Twitter?

No. The network did not have Internet access :(

So I can just port scan every network and get r00t?

All the cool kids are so why not? */s*

On a serious note, port scanning is a gray area because no laws exist for it. While I know we all run around shouting "port scanning is not a crime" with our black hoodies and thirty DEFCON badges on, this may not always be the case. I'm not a lawyer so don't ask me though! :)

Default Credentials = CVE. Lulz.

Yeah, I'm with you. I walked the dinosaur around my room deciding if this is something I should even bother requesting a CVE for. At the end of the day it gave me default raspberry pi credential vibes. I hate to be that guy, but default credentials are always bad, and there really isn't a good excuse to ever use them.

Thanks

- Thanks to MA Lighting for being open to discussing this issue with me even though I'm not a customer and taking the time to relay messages between myself and the dev team.
- Thanks to my good friend Catatonic for listening to me rant a little about this and sending me some references.
- Thanks to you.. Yeah **YOU** for reading this post. I know it wasn't a high-level RCE exploit with a PoC provided but this was a fun one to write and I appreciate you for reading it <3

Penetration-Testing , Infrastructure

penetration-testing cve

Share:

Further Reading

Nov 3, 2019

HackTheBox | Swagshop Walkthrough

I took a small break from doing active machines on HackTheBox while working…

Mar 18, 2022

OSCP Notes & Resources

I passed my OSCP awhile back and I wanted to contribute to the many 'useful notes'…

Apr 24, 2022

Automating Security with CrowdSec

Let's Talk for a Minute Securing infrastructure is a topic that I don't see…

OLDER NEWER