Security Shards

Follow the black rabbit…

CVE-2021-40350 – Christie DWU850-GS Authentication Bypass

This vulnerability that I am going to exploit allows me to create privileged accounts; completely bypassing the need to log in as an admin to create the account. This escalation allows access to the appliance and provides an attacker access to the configuration. This is done by sending a uniquely crafted POST request and inserting an *unique* cookie. This is how it works.

From the image below, you can see that I am sending the following POST request:

 (https://securityshards.files.wordpress.com/2021/08/christie_request1-1.png)

From the command, you can see that the username is **bypassadmin** and the password is **bypass**. I It is also important to note that I also inserted the *unique* cookie to the payload. The Christie does not validate the request as long as it see's this cookie. Usually, sessions are given this cookie and an elevated account forms a session, and destroyed when the session ends.

The next image shows the response of the Christie:

 (https://securityshards.files.wordpress.com/2021/08/christie_response1-1.png)

As you can see, the response came back with the *unique* cookie. Once we refresh the page, you can see the newly created account:

 (https://securityshards.files.wordpress.com/2021/08/christie_login.png)

We can also use the information we sent on the request to authenticate to this elevated user account:

 (https://securityshards.files.wordpress.com/2021/08/christie_access1.png)

As you can see, this vulnerability can leverage an attacker to gain access to a Christie device without having to authenticate. Aside from the security risk, it can disturb the configurations of these devices through the portal and set rogue DHCP servers.

To prevent abuse, I am going to keep the vector private to prevent the flaw from being exploited from malicious actors.

🏷 UNCATEGORIZED