May 10 • Written By James Carroll

SpecoWeb Directory Traversal (CVE-2021-32572)

SpecoWeb (presumably all versions or at least all versions that I have tested) is vulnerable to a directory traversal vulnerability. This vulnerability can be exploited using a browser and Burp Suite.

Appending /../../../../../../../../../etc/passwd at the end of a SpecoWeb URL discloses the hash values of all users. All affected instances that have been tested thus far appear to have just the "root" users hash value. An example of this is shown in the image below.

SpecoWeb homepages that appear to be vulnerable look like the following.

Using this, you can create a quick Shodan query that yields a bunch of vulnerable instances by just searching "Speco Library".

I have reached out to Specko and informed them about this vulnerability and am awaiting a response.

James Carroll

Pivoting with Meterpreter and ProxyChains   Introduction to SILENTTRINITY - Tutorial 2020

Have questions? Add me on LinkedIn and let's meet
root@jamescarroll.me ~

Security Blog