@bertinjoseb Follow
Mar 17 · 5 min read · Listen

Post auth RCE based in malicious LUA plugin script upload SCADA controllers located in Russia

Hello World

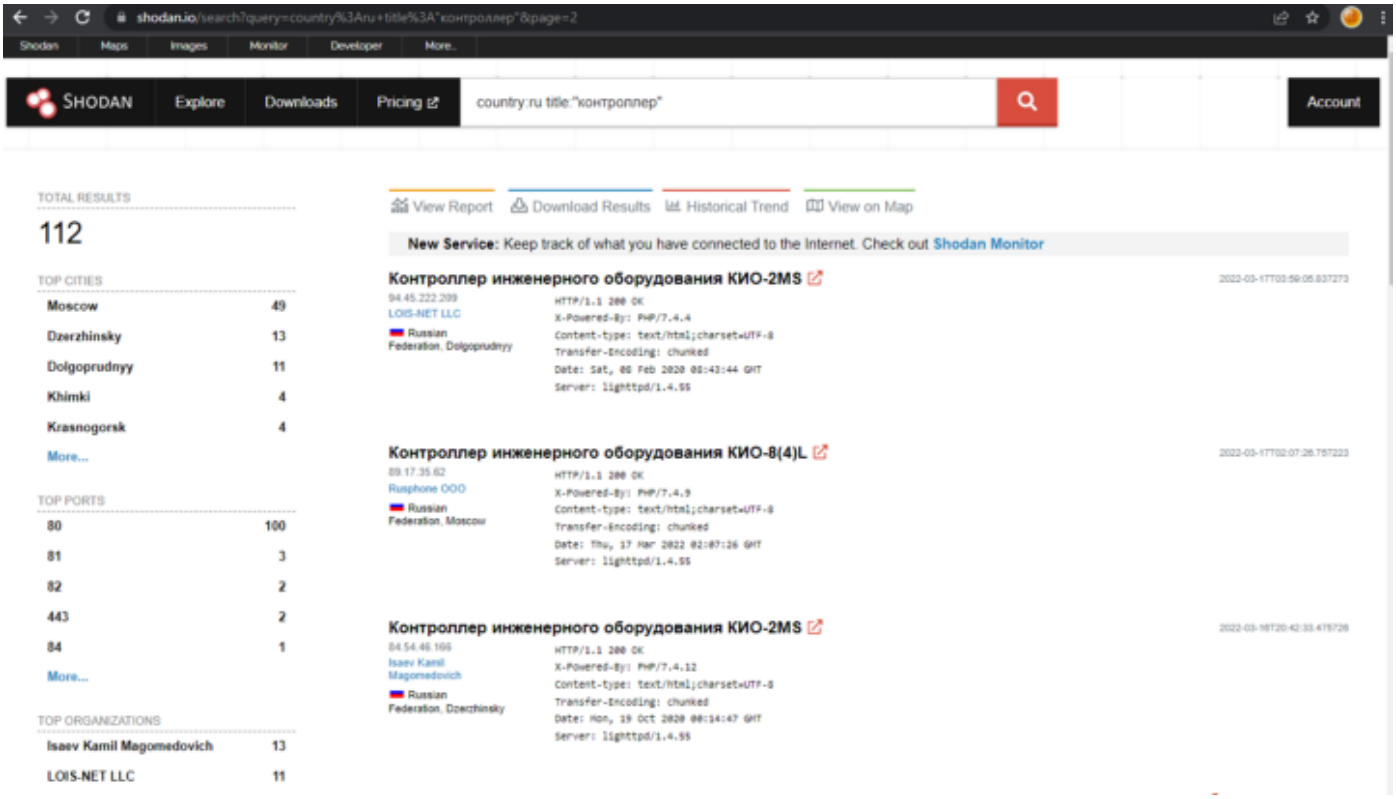
The following is a writeup about a research i did today at morning march 17 2022 , took me 3 hours and no breakfast, after lunch and succesful pwned i'm writing this.

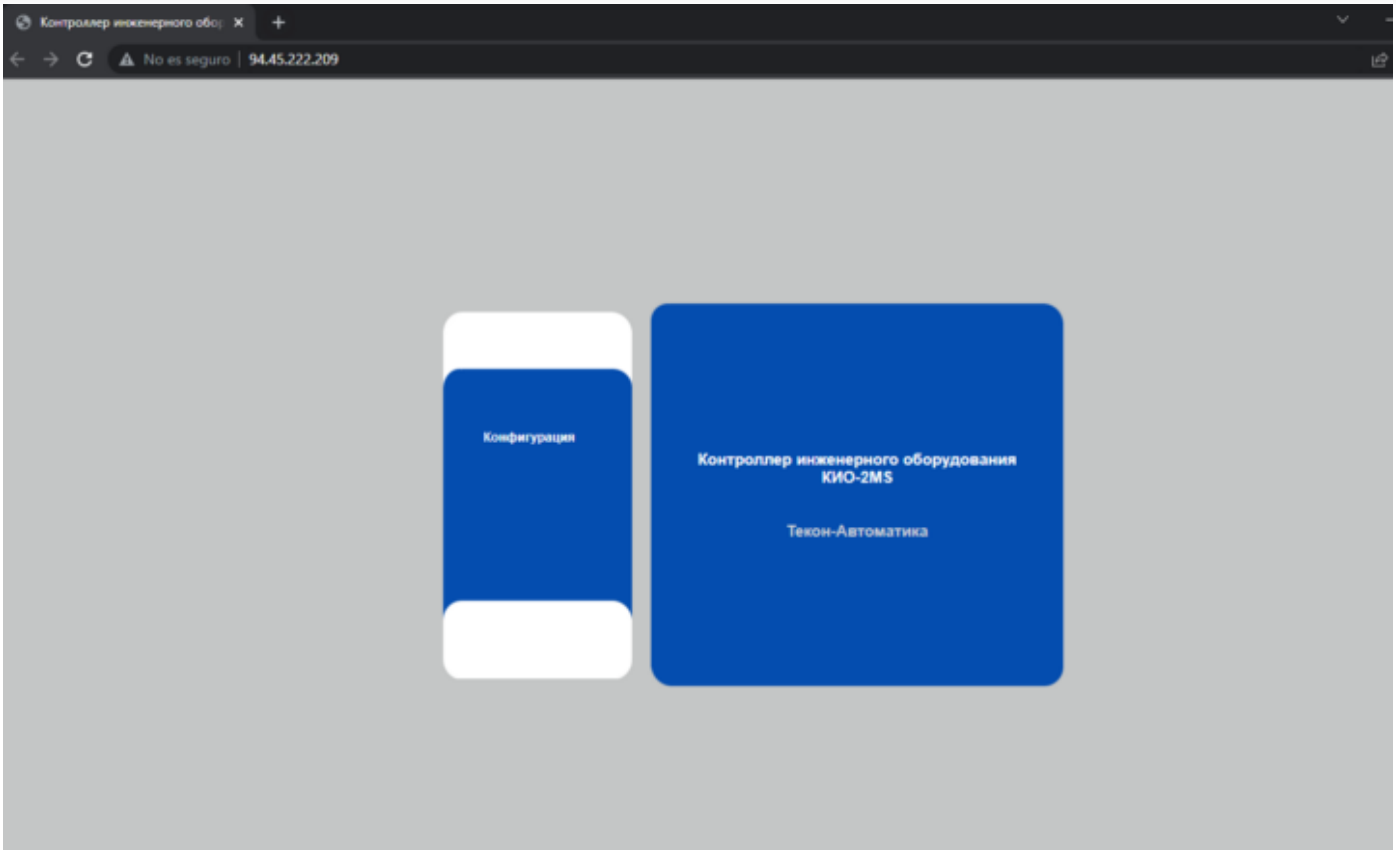
The affected devices are controllers from a russian brand called tekon.ru

enviroments.

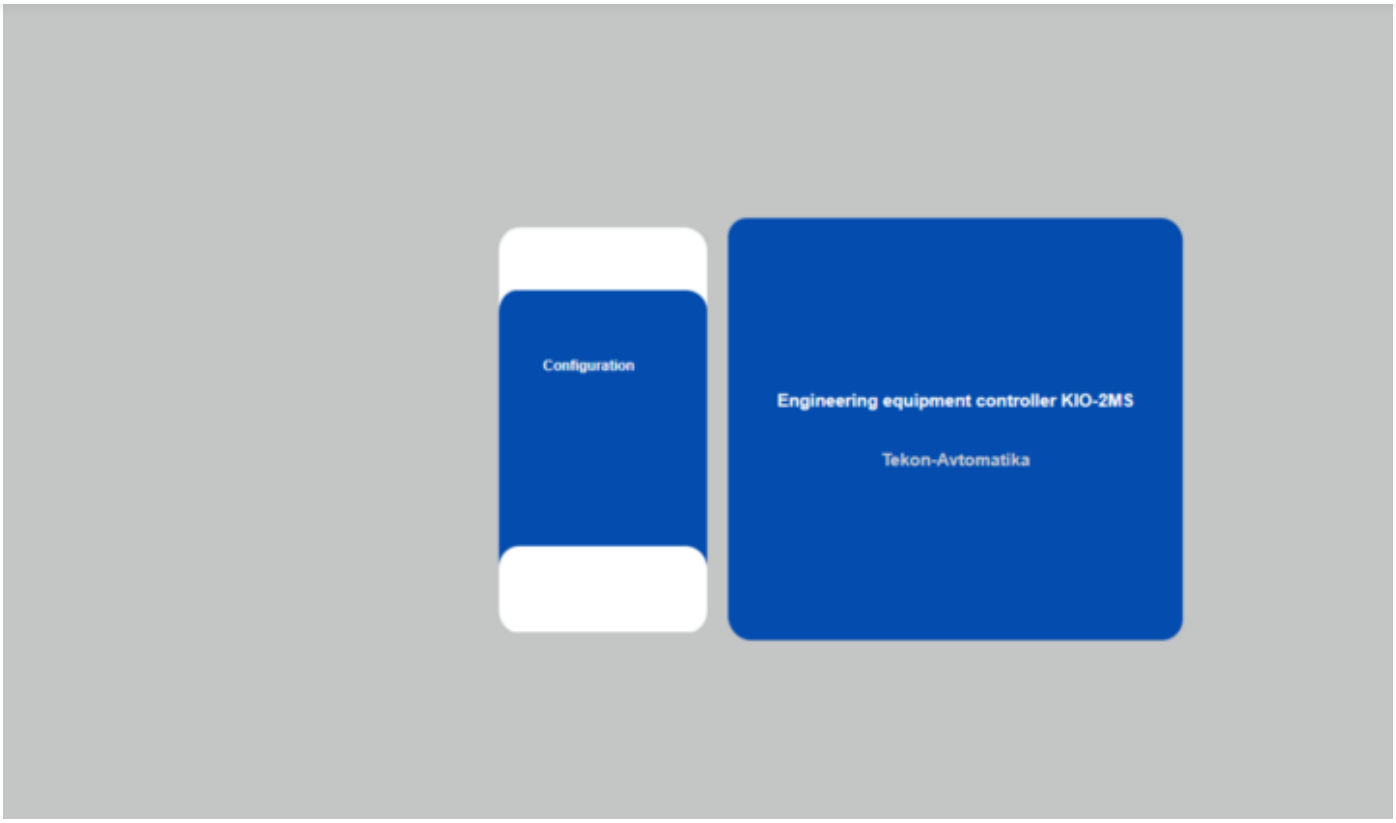
I found more than 100+ devices connected to the internet all them located in Russia exclusively , those devices are running with default credentials almost all of them and anyone can connect to them and perform changes and actions as “admin” only .

https://www.shodan.io/search?query=country%3Aru+title%3A%22%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%BB%D0%B5%D1%80%22&page=2

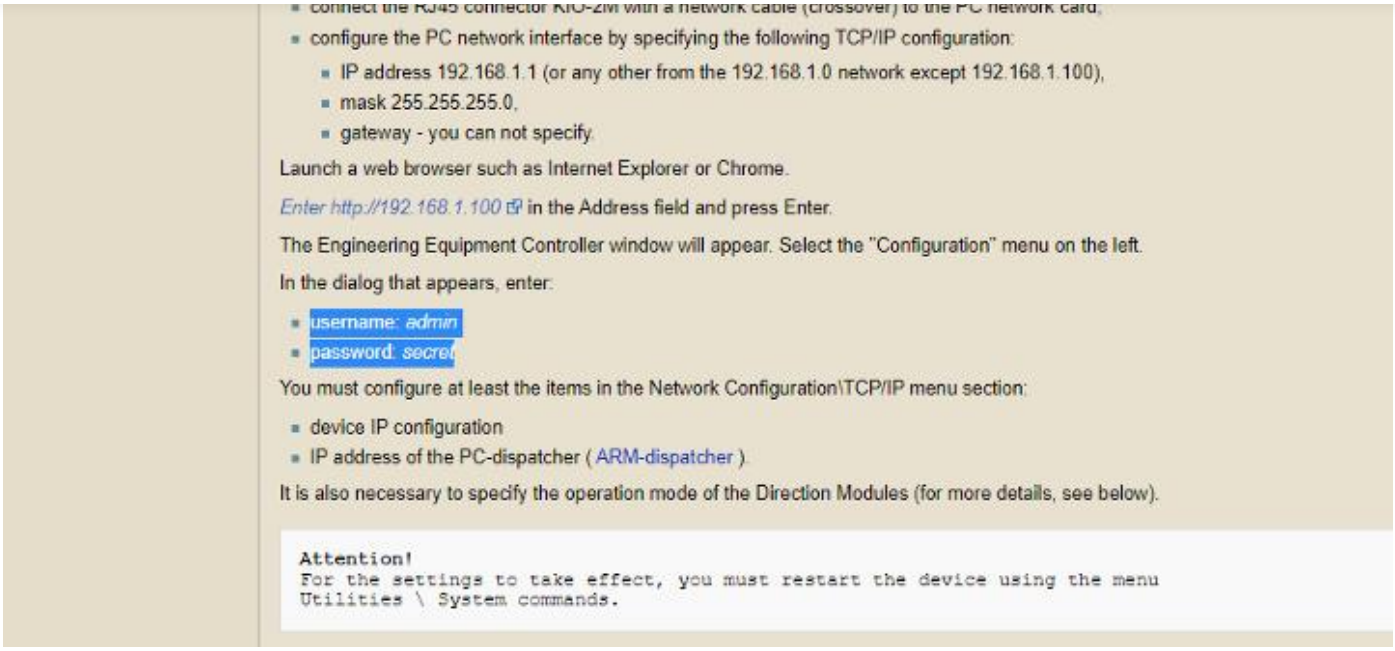




Everything is in russian but don’t worry gogle translate tab is your friend



After some research i found that tekon.ru did a great job put it in manuals firmwares and software related to easy access for anyone interested to take a look , in our case we need the manuals in order to dig for some default credentials , you know... in our case we need to acces somehow someway ..



After translation and reading i found the default credentials which are ***admin:secret*** , trying the first result i was completely in, profit for me!!

Well now i’m in with defaults what can i do here ? and more importantly what kind of priviledges i have at this moment , you can enable the SSH access from the panel or even change the default password , so the engineers are not going to be able to acces again if you do that ...

So, with the SSH access my idea was to confirm what type of priviledges the user admin is running right now, for my surprise the admin user is not root, which is boomer at that point of the research .

Well, this means we can not do any interesting action with the admin user like command execution, we need to escalate privilegdes someway somehow .

After reading all manuals and learn about the device features i noticed there are some documented cgi scripts and some of them are not documented

in the path /srv/www/cgi-bin you can find those scripts , some of them are interesting like the serkill.cgi, you can call it and a process is going to be stoped

Well i was thinking..... if i could upload my custom cgi script i could execute bash, but the user admin doesn't have the permisions, permission is denied.

Mmm.. seriously i need to figure out how to upload my stuff here and execute commands, i knew i was closer.

After reading again the manuls for second time and playing around with the web app i found an interesting module for LUA script plugin upload and execution, just look for the plugin section .

According the manuals you can upload your custom LUA scripts “plugins” and they are going to be executed after you click the save/load button.

I though the following, LUA plugin should be running as root yes or yes , if i could upload a malicious LUA plugin with custom commands those are going to be executed as root and then i could place a custom cgi in /srv/www/cgi-bin path easily bypassing the admin user priviledges.

Ok here we go, open up your notepad++ and write some LUA code , in order to execute OS commands you just need os.excute

Save the LUA malicious plugin/code and create a .TAR file with 7 zip in windows

Upload the malicios LUA plugin

Then press save/load

called *log.cgi*

invoke log.cgi

After upload the malicious LUA plugin just invoke log.cgi script , go to the bottom and you will see the output for the obscure LUA plugin

BOOM !! WE GOT RCE AND PRIVILEDGE ESCALATION 😎

NOW WE ARE ROOT !!!

1337

Let's try with cat /etc/passwd

Yeah !! there you go 😎 gimme the shit

cat /etc/passwd

Well i got RCE and privilege escalation from an admin user to root , now we can do whatever, more critically those devices can be shut down at once the 100 creating an impact in russian scada systems , remotely.

From this point now we can create custom cgi files and call them from cgi/bin path and do whatever .

You can follow on twitter for more “on the fly” research and pwn delivery @bertinjoseb

Thanks