Sysax-MultiServer-6.90-Multiple-Vulnerabilities

Multiple vulnerabilities were discovered in Sysax Multi Server 6.90

*** Vendor was informed on May 19th, 2020 but I have not received any feedback ***

1) Insecure Permissions and Information Disclosure via error handling
::: CVE-2020-13227 :::

Description:
An attacker can determine the username (under which the web server is running) by triggering an invalid path permission error. This bypasses the fakepath protection mechanism.

PoC:
http://192.168.88.131/scgi?sid=7d2ec36cd2f0a42929a5672c9cc5f0320a666155&pid=transferpage2_name1_(folder_where_you_don't_have_permissions).htm

E.g
http://192.168.88.131/scgi?sid=7d2ec36cd2f0a42929a5672c9cc5f0320a666155&pid=transferpage2_name1_johnfolder.htm

PoC screen: https://pasteboard.co/J9eF12G.png

2) Reflected Cross Site Scripting (XSS)
::: CVE-2020-13228 :::

Description:
There is a reflected XSS via the /scgi sid parameter.

PoC:
http://192.168.88.131/scgi?sid=684216c78659562c92775c885e956585cdb180fd<script>alert("XSS")</script>&pid=transferpage2_name1_fff.htm

PoC Screen: https://pasteboard.co/J9eE2GQ.png

3) Incorrect Access Control - Session Fixation
::: CVE-2020-13229 :::

Description:
A session can be hijacked if one observes the sid value in any /scgi URI, because it is an authentication token.

PoC:
When the user is logged on, URI something like this is generated: http://192.168.88.131/scgi?sid=684216c78659562c92775c885e956585cdb180fd&pid=mk_folder1_name1.htm
Considering that "sid" parameter is the auth token of the user (passed in GET), simply replacing the complete URI in any session (changing the browser), you will have the access to that user without the necessity to perform login.