Mercury MER1200 Router v1.0.1 RCE

the function add_server_service in /usr/lib/lua/luci/controller/admin/pptp_server.lua

```
function add_server_service(http_form)
        local content = luci.json.decode(http_form.data)
        content = content.params.new
        local name = nil
        local getRet = {}

        --check the data legality
        if not check_option_legality(content, "server") then
                return false,err.ERR_VPN_INVALID_PARAMS
        end

        if not content.server then
                content.server = _get_available_servername()
        else
                uci_r:foreach("pptp-server","pns",
                        function(section)
                                if section["server"] == content.server then
                                        gdb("server name conflicted")
                                        return false,err.ERR_COM_TABLE_ITEM_UCI_ADD
                                end
                        end
                )
        end
        --check if the bind WAN exists in config file
        uci_r:foreach("pptp-server","pns",
                function(section)
                        if section["bindif"] == content.bindif then
                                gdb("service already exists in this wan interface")
                                return false,err.ERR_COM_TABLE_ITEM_UCI_ADD
                        end
                end
        )
        local ret=uci_r:section("pptp-server","pns",nil,content)
        if not ret then
                return false,err.ERR_COM_TABLE_ITEM_UCI_ADD
        end

        if not uci_r:commit("pptp-server") then
                return false,err.ERR_COM_UCI_COMMIT
        end

        local pptp_cmd=string.format("lua /lib/pptp/pptp_process_manager.lua")
        sys.fork_call(pptp_cmd)

        --directly pass those params to shell
        local cmd = string.format("/lib/pptp/add-service.sh %s %s %s %s %s",content.server,content.bindif,content.enable,content.mppe
        sys.fork_exec(cmd)
        ifs.update_if_reference(content.bindif,1)
        dhcp_m.lan_settings_set_manual_mode()
        userconfig.cfg_modify();
        return content
end
```

In lines 397,398

```
        local cmd = string.format("/lib/pptp/add-service.sh %s %s %s %s %s",content.server,content.bindif,content.enable,content.mppe
        sys.fork_exec(cmd)
```

Directly splice parameters content.server to the command.

In line 359

```
        if not check_option_legality(content, "server") then
                return false,err.ERR_VPN_INVALID_PARAMS
        end
```

function check_option_legality

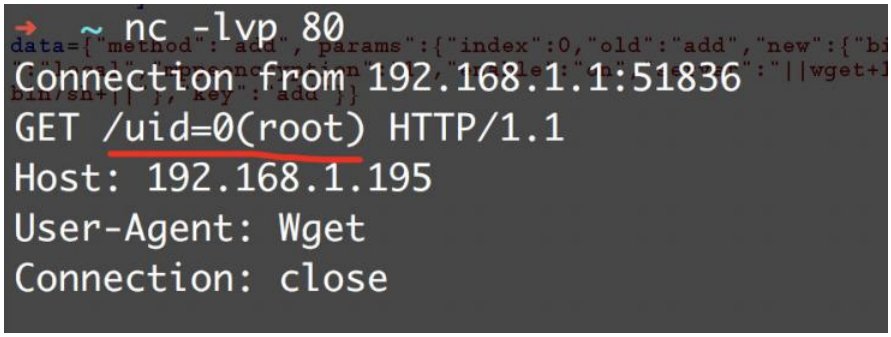
```
        elseif data_type == "server" then
                if data.authtype ~= "local" then
                        return false
                end

                if not dt_m.iface(data.bindif) then
                        return false
                end

                if not dt_m.bool(data.enable) then
                        return false
                end

                if not dt_m.bool(data.mppeencryption) then
                        return false
                end
        end
```

There is no judgment on the parameters server, which results in that when adding a PPTP server, the command can be executed by manually changing the package.



The id command was successfully executed and the permission is root