D-link DSH-C310FW predictable password

firmware information

Vendor: D-link

Firmware: D-link DSH-C310FW

Version: DSH-C310FW1.05

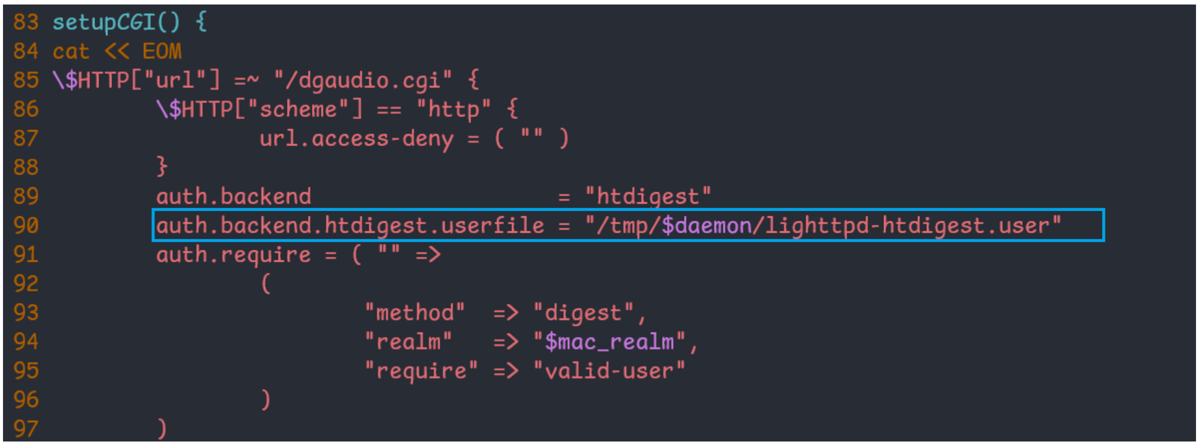
Firmware support URL: https://www.dlink.ru/mn/products/1433/2206.html

Description

D-link DSH-C310FW is found to have predictable password. Unauthenticated attackers can send malicious packet containing predictable credential and gain administrative privilege.

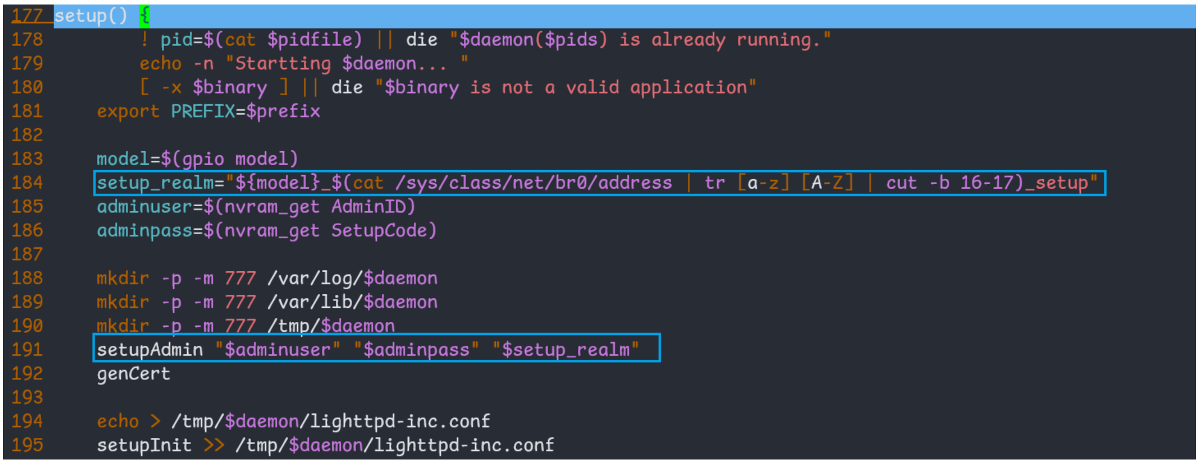
Detail

During firmware initialization, `sbin/lighttpd.sh` will be executed to initialize web server's running environment. The firmware uses `lighttpd` as webserver backend and uses configuration file `lighttpd-htdigest.user` as authenticated file.



```
setupCGI() {
cat << EOM
\$HTTP["url"] =~ "/dgaudio.cgi" {
        \$HTTP["scheme"] == "http" {
                url.access-deny = ( "" )
        }
        auth.backend                   = "htdigest"
        auth.backend.htdigest.userfile = "/tmp/$daemon/lighttpd-htdigest.user"
        auth.require = ( "" =>
                (
                        "method"  => "digest",
                        "realm"   => "$mac_realm",
                        "require" => "valid-user"
                )
        )
```

The following function `setup` contains the initialization of firmware's password. It uses `setup_realm` as the third argument and transfer it to function `setupAdmin`. Notice that `setup_realm` is predictable since it uses the firmware's model name, MAC address and constant string "_setup" as input, which can be effectively guessed or acquired by attackers. (For example, attackers can get the MAC address of the firmware through web packet sniffing)



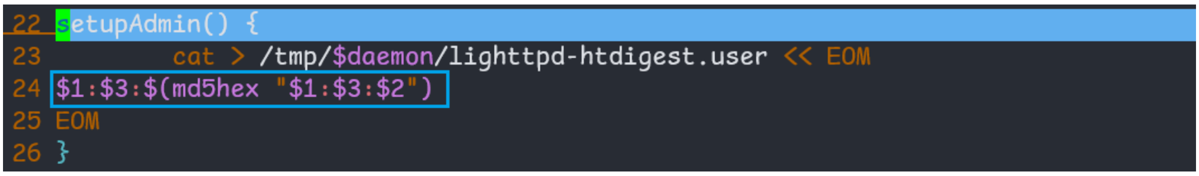
```
setup() {
        ! pid=$(cat $pidfile) || die "$daemon($pids) is already running."
        echo -n "Startting $daemon... "
        [ -x $binary ] || die "$binary is not a valid application"
    export PREFIX=$prefix

    model=$(gpio model)
    setup_realm="${model}_$(cat /sys/class/net/br0/address | tr [a-z] [A-Z] | cut -b 16-17)_setup"
    adminuser=$(nvram_get AdminID)
    adminpass=$(nvram_get SetupCode)

    mkdir -p -m 777 /var/log/$daemon
    mkdir -p -m 777 /var/lib/$daemon
    mkdir -p -m 777 /tmp/$daemon
    setupAdmin "$adminuser" "$adminpass" "$setup_realm"
    genCert

    echo > /tmp/$daemon/lighttpd-inc.conf
    setupInit >> /tmp/$daemon/lighttpd-inc.conf
```

In function `setupAdmin`, it uses the third argument (which is the predictable `setup_realm`) as password(according to the specification of lighttpd authentication mod manual: https://redmine.lighttpd.net/projects/lighttpd/wiki/mod_auth). So the firmware acutally uses predictable password for authentication.



```
setupAdmin() {
        cat > /tmp/$daemon/lighttpd-htdigest.user << EOM
$1:$3:$(md5hex "$1:$3:$2")
EOM
}
```