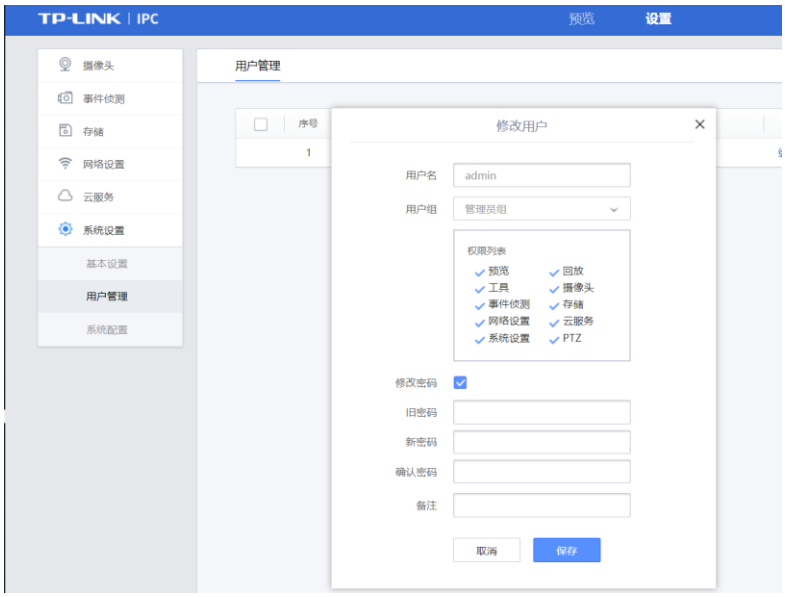
Vulnerability Title: Hard-coded private key of TP-Link IPC leaked.
Vulnerability Description: The private keys of IPC is hard-coded in the firmware, which could decrypt the password of IPC to plain text.
Required Affected Versions: 1.0.8 Build 210105 Rel.65035n
Tested Platform: TL-IPC42C-4 5.0

When a user try to change his password, he need to input old password and new password.

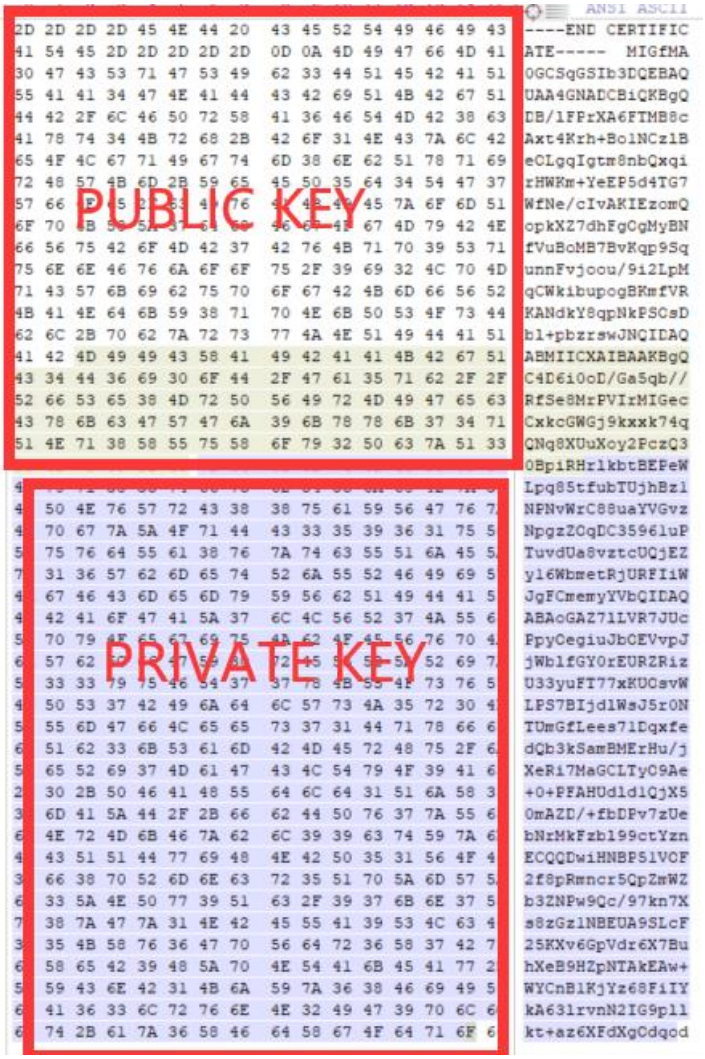


The JS script encrypts the new password by RSA pubilc key.
"""-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4D6i0oD/Ga5qb//RfSe8MrPVIrMI
GecCxkcGWGj9kxxk74qQNq8XUuXoy2PczQ30BpiRHrlkbtBEPeWLpq85tfubTUjhBz1NPNvW
rC88uaYVGvzNpgzZOqDC35961uPTuvdUa8vztcUQjEZy16WbmetRjURFIiWJgFCmemyYVbQ
IDAQAB
-----END PUBLIC KEY-----"""

```
},
changeDefaultPwd: function(a, b) {
    var c = orgAuthPwd(a);
    $.tmpPwdMD5 = $.getPwdMD5($.rootName, a);
    var e = {
        method: "do",
        set_password: {
            password: c,
            username: $.rootName,
            ciphertext: $.encryptPwd(a)
        }
    };
    $.accountStatus.logoutHandle = !1;
    $.sendAjaxReq("", e, function(a) {
        var e = a[ERR_CODE];
        if (ENONE == e || ESUPERPWDSUCCESS == e) {
            $.authRltObj.authStatus = !0;
            $.setLg($.rootName, c, "");
```

web-static/lib/jquery-1.10.1.js

However, this pair of keys are hard-coded at firmware, as following shows:



And the private key is:

"""-----BEGIN RSA PRIVATE KEY-----

MIICXAIBAAKBgQC4D6i0oD/Ga5qb//RfSe8MrPVIrMIGecCxkcGWGj9kxxk74qQNq8XUuXo
y2PczQ30BpiRHrlkbtBEPeWLpq85tfubTUjhBz1NPNvWrC88uaYVGvzNpgzZOqDC35961uPTu
vdUa8vztcUQjEZy16WbmetRjURFIiWJgFCmemyYVbQIDAQABAoGAZ7lLVR7JUcPpyOegiu
JbOEVvpJjWblfGY0rEURZRizU33yuFT77xKUOsvWLPS7BIjdlWsJ5r0NTUmGfLees71Dqxfed
Qb3kSamBMErHu/jXeRi7MaGCLTyO9Ae+0+PFAHUdld1QjX50mAZD/+fbDPv7zUebNrMkFz
bl99ctYznECQQDwiHNBP51VOF2f8pRmncr5QpZmWZb3ZNPw9Qc/97kn7Xs8zGz1NBEUA9
SLcF25KXv6GpVdr6X7BuhXeB9HZpNTAkEAw+WYCnB1KjYz68FiIYkA63lrvnN2IG9pllkt+a
z6XFdXgOdqodoi3pWvmhkU55Z2N0okuGjm93qO1pebC3JcPwJAOsn+8Yms2LFoILnXj6UtgP
LHc8id32Wjb5dT6EyR0rJ2louYbe4F5pBxGIukPKdpB94Ld9SAivRLQWW4r2jgxQJBAJo1+D1
nj+Rd7PuPLXfmyRGVcQrpC7m22vDfXUDqOeBNZXX1Ns0Y0lBUl3sAeaNhn8ggls2QzxlMon
stt4EIUrMCQCgOhLJ1SoUw1RE+b3x5hpuibFpiknX9MAjNxMJ1vHQFgsYTIVlD9LdHc/+nGb
eXhzi0BJ2h3R5tmQmIseOs9f0=

-----END RSA PRIVATE KEY-----"""

And the data is transferred by HTTP.
Therefore the passive attacker could easily eavesdrop and decrypt the password of user.

Here is the example of the attack.