

Projektstudium Pentesting

Moritz Rupp, Marius Hald, Lukas Heinzelmann, Dean Basic

Inhalt

- Projektvorstellung
- Zielgerät
- Vorgehen
- Scan
- Berichte

Projektvorstellung

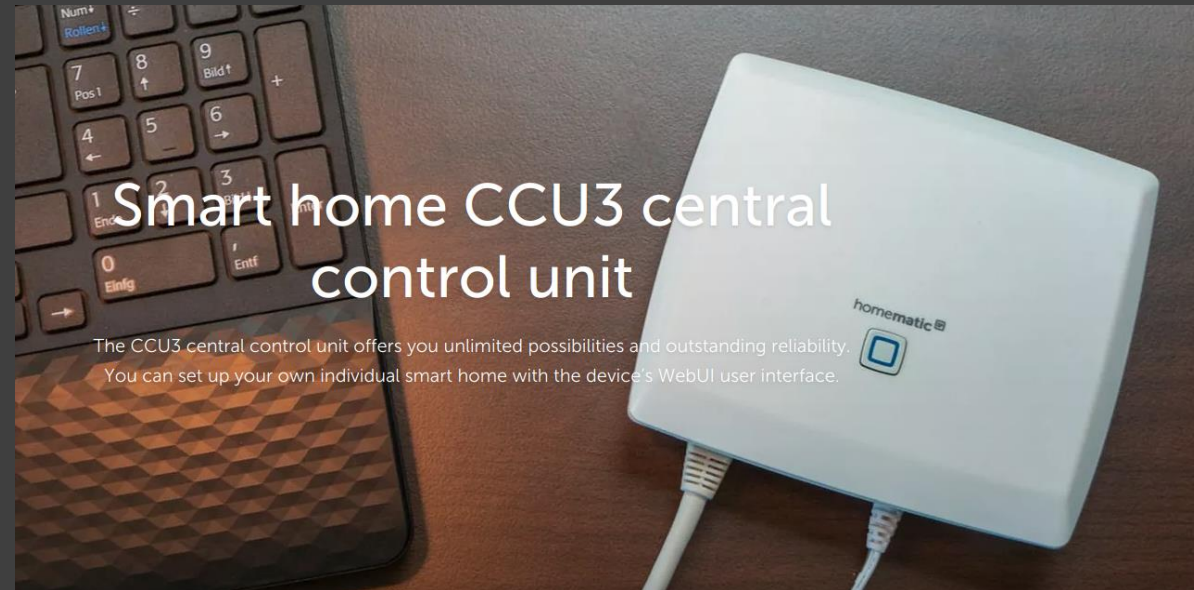
- Durchführung eines Penetrationstestes unter realen Bedingungen
- Anwendung auf ein reales Produkt/System
- Erstellung eines Reports
- Vorstellung bei Auftraggeber

Zielgerät Vorstellung

- Smart Home Zentrale

Heimautomatisierung

- Steuereinheit für Verbundene Geräte
 - Heizung, Rolläden, Türen, Fenster, Beleuchtung
- Bietet Weboberfläche





- Homematic nutzt ein verbauten Raspberry Pi 3b2015
- Custom board mit Antenne zugebaut
- Leicht zugänglich

Weboberfläche

POWNED

HomeMatic
homematic IP **Anmelden**

Admin

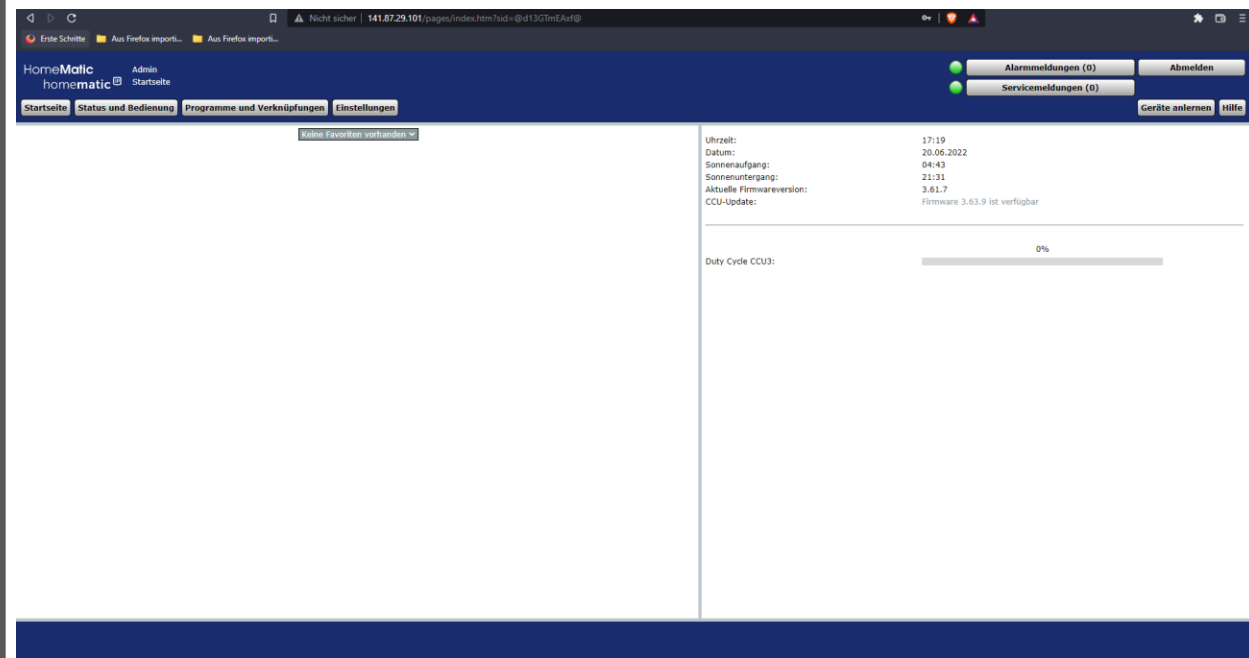
guest

user

**Bitte geben Sie Ihren
Benutzernamen ein.**

**Bitte geben Sie Ihr Passwort
ein.**

Anmelden



Vorgehen

- Planung
 - Scope
 - Ziele
 - Scan
 - Manuelle/Automatische Vulnerability scanner
- Nmap, Dirbuster, OWASP ZAP, Curl, Shodan
- Minimierung der Befunde
 - Austestung der Schwachstellen
 - Analyse und Report

Planung

Scope: Testen der
Geräte Hardware und
Software auf Schutzziele
der
Informationssicherheit

Greybox ansatz

Szenario abhängig

Ziele: Feststellung und
Verbesserung des
Sicherheitszustandes

Scan

- Reconnaissance mit tools wie dig, nmap, curl

```
sleven parrot ~ dig 141.87.29.101

; <==> DiG 9.16.27-Debian <==> 141.87.29.101
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49054
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;141.87.29.101.                IN      A
;
;; AUTHORITY SECTION:
;                               900      IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2022072500 1800 900 604800 86400
;
;; Query time: 76 msec
;; SERVER: 141.87.114.201#53(141.87.114.201)
;; WHEN: Mon Jul 25 15:13:42 CEST 2022
;; MSG SIZE rcvd: 117
```

Fingerprinting

```
sleven parrot ~ curl -I 141.87.29.101
HTTP/1.1 510
Accept-Ranges: bytes
Cache-Control: private, no-cache, must-revalidate, no-transform, max-age=0
Content-Type: text/html; charset=iso-8859-1
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Robots-Tag: none
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
Date: Mon, 25 Jul 2022 13:34:57 GMT
```

Fehlender HTTP Security header

- **Content-Security-policy (csp):**

Über diese kann gesteuert werden, welche Inhalte aus welcher Quelle Zugelassen werden. Hierüber können Javascript Angriffe wie XSS etc. Verhindert werden.

Empfehlung:

- default-src 'self/none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';base-uri 'self';form-action 'self'

- **Strict transport Security:**

- Festlegung zu Webseiten Aufrufe ausschließlich über HTTPS.
- Verhinderung von MiM Angriffen

Empfehlung:

- Header set Strict-Transport-Security "max-age=31557600"
env=HTTPS

Portscan

```
sleven parrot ~ nmap -sC -sV 141.87.29.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 15:12 CEST
Nmap scan report for 141.87.29.101
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.8 (protocol 2.0)
80/tcp    open  http     lighttpd
|_http-title: HomeMatic WebUI
443/tcp   open  ssl/http lighttpd
|_http-title: HomeMatic WebUI
| ssl-cert: Subject: commonName=ccu3-webui/organizationName=HomeMatic/countryName=DE
| Not valid before: 2022-03-23T15:55:18
|_Not valid after:  2032-03-20T15:55:18

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.23 seconds
```

Enumeration

```
sleven parrot ➔ gobuster dir --wordlist /usr/share/wordlists/dirb/big.txt -u 141.87.29.101

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://141.87.29.101
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/07/25 18:04:11 Starting gobuster in directory enumeration mode

/addons (Status: 301) [Size: 0] [--> http://141.87.29.101/addons/]
/bin (Status: 403) [Size: 345]
/bin_install (Status: 403) [Size: 345]
/bin_old (Status: 403) [Size: 345]
/binaries (Status: 403) [Size: 345]
/bind (Status: 403) [Size: 345]
/bing (Status: 403) [Size: 345]
/binary (Status: 403) [Size: 345]
/bingen (Status: 403) [Size: 345]
/bingo-scotland (Status: 403) [Size: 345]
/bingo (Status: 403) [Size: 345]
/binky (Status: 403) [Size: 345]
/bins (Status: 403) [Size: 345]
/binsource (Status: 403) [Size: 345]
/binsrc (Status: 403) [Size: 345]
/bootcamp (Status: 403) [Size: 345]
/boot (Status: 403) [Size: 345]
/booth (Status: 403) [Size: 345]
/bootsie (Status: 403) [Size: 345]
/boots (Status: 403) [Size: 345]
/etc (Status: 403) [Size: 345]
/favicon.ico (Status: 200) [Size: 1150]
/pda (Status: 301) [Size: 0] [--> http://141.87.29.101/pda/]
/usrmgr (Status: 403) [Size: 345]
/usrs (Status: 403) [Size: 345]
/usr (Status: 403) [Size: 345]
/~sys- (Status: 403) [Size: 345]
```

Outdated jquery Versionen

- http://141.87.29.101/webui/js/extern/jquery.js?_version_=2.0pre1

- Führen zu CVE-2020-11023 und CVE-2020-11022
- Empfehlung: Updaten auf neuste jquery Version

CVE-2020-11023 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Fehlende Anti CSRF Tokens

- <http://141.87.29.101/login.htm>
- Umgehung von Same origin policy
- Cross-site request forgery möglich
- Empfehlung
 - Verwendung eines anti-CSRF Packetes

Session ID Rewrite

- Bei Anmeldung wird eine Session ID angelegt.

```
141.87.29.101/pages/index.htm?sid=@zUKL0aPYEB@
```

- Diese wird über URL rewrite erzeugt.
- Kann somit in Server logs, oder Browser cache/verlauf einsehbar werden.
- Nach Fenster Schließung ist Session ID 300 Sekunden lang gültig.

Empfehlung:

- Session ID in einem Cookie speichern
- Gültigkeit nach Fensterschließung auf 180 sekunden reduzieren



Brute Force

- Keinen Cooldown bei Passwort Eingabe
- Admin Passwort wird nie verändert
- Keine Benachrichtigung mehrmaliger falsch Eingabe
- Passwort mit Zufallsgenerator erstellen
- Cooldown einrichten
- Besitzer des Homematic Geräts benachrichtigen

Skripte hochladen

- Skripte können innerhalb der CCU3 hochgeladen werden
- Können Schadsoftware beinhalten
- Skripte müssen erst getestet werden
- Keine unbekannten Skripte herunterladen

Software Update

- Software Updates nicht automatisch
- Update Vorgang kann sehr lange dauern
- Manche Geräte funktionieren nach Update nicht mehr
- Updates können nur vom Techniker durchgeführt werden

Remote Code Execution

- Aktuell keine bekannten Schwachstellen
- Wichtig Version >3.56.6
- Letzte bekannte kritische Schwachstelle CVE-2019-9583
- Meist wird die SessionID wird ausgelesen

Replay Angriff

- Bei einem Replay Angriff werden die Signale zur Steuerung von diversen Geräten wie z.B. Autoschlüsseln, Garagentoröffnern oder Smart Home Geräten aufgezeichnet und zu einem späteren Zeitpunkt wieder Abgespielt um diesen Steuervorgang erneut auszulösen
- Voraussetzung ist, dass dieser nicht bereits durch Rolling Code, Nonces oder ähnliches vorgebeugt wird

Replay Angriff

<https://www.nooelec.com/store/sdr/sdr-receivers/nesdr-smart-xtr-sdr.html>



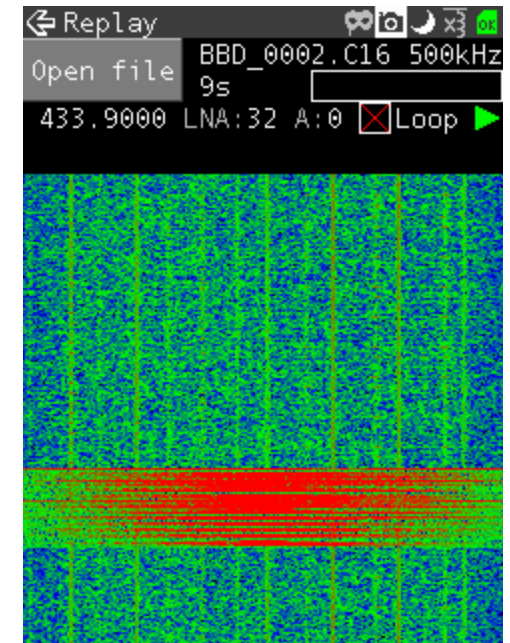
Unser verwendetes SDR
(Rx only!)

<https://greatscottgadgets.com/hackrf/one/>



SDR mit Rx/Tx Fähigkeit

<https://www.rtl-sdr.com/tag/replay-attack/>



HackRF mit Portapack

- Empfehlung: Nicht immer
das Selbe Signal zur
Steuerung verwenden

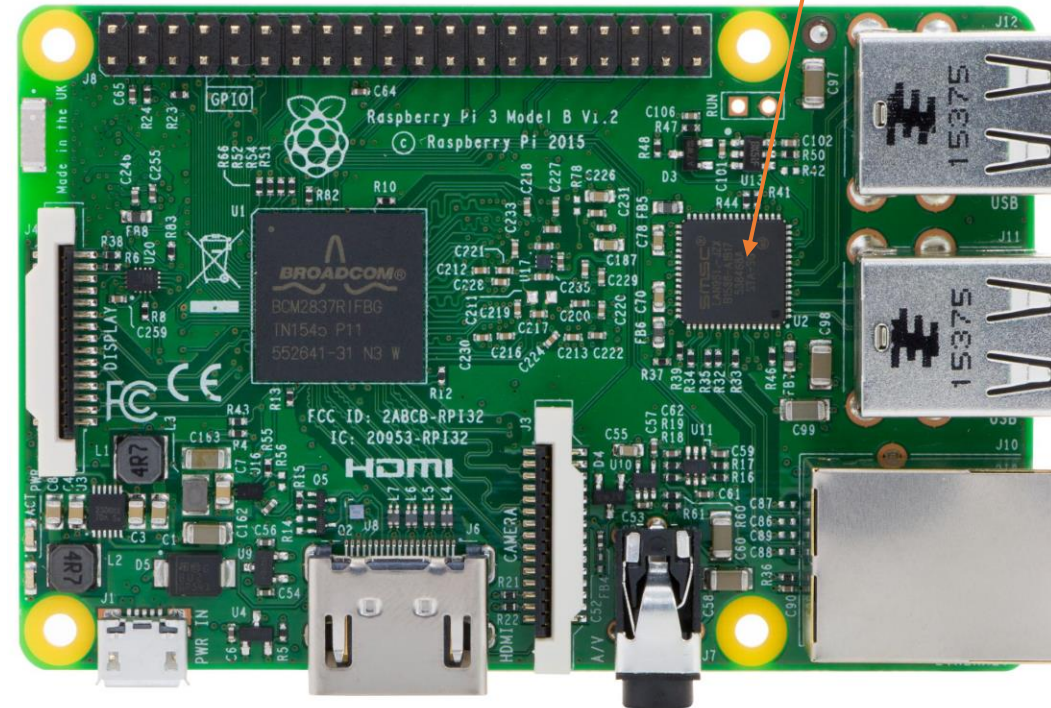
Usb Killer

<https://scheible.it/usb-killer-rechner-zerstoeren/>



Der innere Aufbau eines Usb Killers

<https://de.famell.com/raspberry-pi/raspberrypi3-modb-1gb/sbc-raspberry-pi-3-model-b-1gb/dp/2525225>



Raspberry Pi 3B, wie im CCU-3 verbaut

Usb/Ethernet IC

Empfehlung:
Überspannungsschutz auf
Datenleitungen oder Gerät
unzugänglich machen

SD-Karte mit Software

<https://www.otto.de/p/sandisk-ultra-microsdxc-64gb-speicherkarte-64-gb-120-mb-s-lesegeschwindigkeit-1461576777/#variationId=1461576778>



SD-Karte auf der die
Software gespeichert ist

Empfehlung: Software
Verschlüsseln, Softwarehash
Verifizierung und Passwörter
nur mit gesalteten Hashes
abspeichern