Bericht

Penetrationstest des Homematic CCU-3

Im Auftrag der SySS GmbH

Ansprechpartner: Tobias Jäger

Durchgeführt von der Hochschule Albstadt-Sigmaringen

Testzeitraum

29.03.2022 - 26.07.2022

Datum: 26.07.2022

Verantwortliche: Moritz Rupp, Dean Basic, Marius Hald, Lukas Heinzelmann

Legal Notice

Dieses Dokument enthält sensible und vertrauliche Informationen, welche nur für die SySS GmbH zugänglich sind. Missbrauch bzw. die nichtautorisierte Vervielfältigung dieses Dokuments ist untersagt.

Der Penetrationstest wurde von einem Team der Hochschule Albstadt-Sigmaringen durchgeführt. Alle gefundenen und getesteten Schwachstellen sind verifizierbar.

Das Testteam übernimmt keine Haftung bei entstehenden
Schäden, die nicht durch das Testteam zu verantworten sind.

Inhaltsverzeichnis

1 Executive Summary

Dieses Dokument beschreibt die Ergebnisse des Penetrationstests für die SySS GmbH. Zweck des Penetrationstest war es ein Überblick über Sicherheit und Konfiguration des Gerätes 'Homematic' zu bekommen. Dieses dient als Zentrale für Smart-home Geräte und steuert somit alle verbundenen Einheiten wie Heizkörper, Lichter, Türen etc. Für die Verwaltung wird eine Weboberfläche bereitgestellt.

Der Penetrationstest simuliert einen böswilligen Angriff mit dem Ziel:

- Festzustellen, ob ein Angreifer sensitive Daten der Zentrale bzw. des Betreibers abgreifen kann
- Die Auswirkungen einer Sicherheitslücke auf Verfügbarkeit, Vertraulichkeit und Integrität der Anwendung.

Die Angriffe wurden unter verschiedenen Szenarien wie dem Angriff von außen als auch durch interne Kompromittierungsversuche durchgeführt. Dies gleicht einem Greybox Ansatz.

2 Scope

Im Rahmen des Untersuchungsauftrages wurde ein vollständiges Gerät in Form der Homematic CCU 3 bereitgestellt. Dieses wurde zu Testzwecken für einen normalen Gebrauch konfiguriert und aufgesetzt. Des Weiteren wurden Anmeldedaten für einen Administrationsaccount der Weboberfläche zur Verfügung gestellt. Mit diesen ist es möglich alle Verwaltungsaufgaben sowie Rechte zu nutzen. Auch können weitere Nutzer mit weniger Berechtigungen angelegt werden.

Der Penetrationstest wird zum einen die Gerätehardware testen und zudem die Software in Form der Benutzeroberfläche bzw. Webanwendung. Hierbei wird untersucht, ob die Schutzziele der Informationssicherheit in Form von Vertraulichkeit, Verfügbarkeit und Integrität beeinträchtigt oder verletzt werden. Netzwerktests werden aufgrund des fehlenden Szenarios nicht berücksichtigt.

3 Summary of Results

Im Verlauf des Penetrationstestes konnten mehrere Sicherheitslücken festgestellt werden. Darunter befindet sich eine akute Bedrohung (vgl. 5 Risikobewertung). Des Weiteren wurden 3 Befunde mit mittleren Bedrohungsstufen ausfindig gemacht (vgl. 5 Risikobewertung). Niedrige Bedrohungen weisen 6 Befunde auf (vgl. 5 Risikobewertung)

Es lässt sich festhalten das der generelle Sicherheitszustand ausreichend ist, jedoch abhängig von dem Nutzungsszenario Optimierungen benötigt.

4 Zeitplan

Das Kick-Off Meeting fand am 22. März 2022 statt. Die Abschlusspräsentation wurde für den 27. Juli 2022 datiert. Der Zeitraum der Tests betrug achtzehn Wochen.

5 Risikobewertung

Risiko	Feststellung	Empfehlung	Referenz
H 1.1	Replay Angriff	Signalübertragung mittels einmaliger Signale (Nonces) oder zusätzlicher Zeitstempelübertragung da sämtliche Zeitstempel nie wieder auftreten	9.5 Seite 18
M 1.1	Brute-Force Anfälligkeit	Cooldown nach mehrmaliger falsch Eingabe, Benachrichtigung wenn das Passwort zu oft falsch eingegeben wurde	9.1 Seite 15
M 2.1	Updates nur durch Techniker möglich	Der Updatevorgang sollte auch Besitzer durchgeführt werden können. Falls ein Update Sicherheitsrelevant ist	9.3.2 Seite 16
M 3.1	Softwareversion unter 3.59.6 Anfälligkeit für RCE.	Homematic CCU3 vor Inbetriebnahme immer updaten. Während des Betriebs sollte das Gerät immer die aktuelle Softwareversion besitzen.	9.3.2 Seite 16
L 1.1	USB-Killer D.O.S	Gerät nicht zugänglich Platzieren oder auf der Platine einen Überspannungsschutz platzieren	9.6 Seite 19
L 2.1	Software auf SD-Karte unverschlüsselt	Software verschlüsseln und ggf. Hash oder Prüfsummenabgleich Passwörter nicht ohne Salt speichern	9.6 Seite 19
L 3.1	SSH Zugang	SSH Zugang nach Einrichtung prüfen und Zugangsdaten ändern.	9.7 Seite 19
I 1.1	Skripte hochladen	Skripte müssen erst getestet werden, bevor sie hochgeladen werden dürfen	9.2 Seite 15
I 2.1	Veraltete Firmware	Ein Firmwareupdate sollte als erstes vom Techniker durchgeführt werden.	9.4 Seite 17
I 2.2	Update-verfahren vereinfachen	Das Softwareupdateverfahren muss vereinfacht werden.	9.3.1 Seite 16

6 Hard- und Softwareinformation

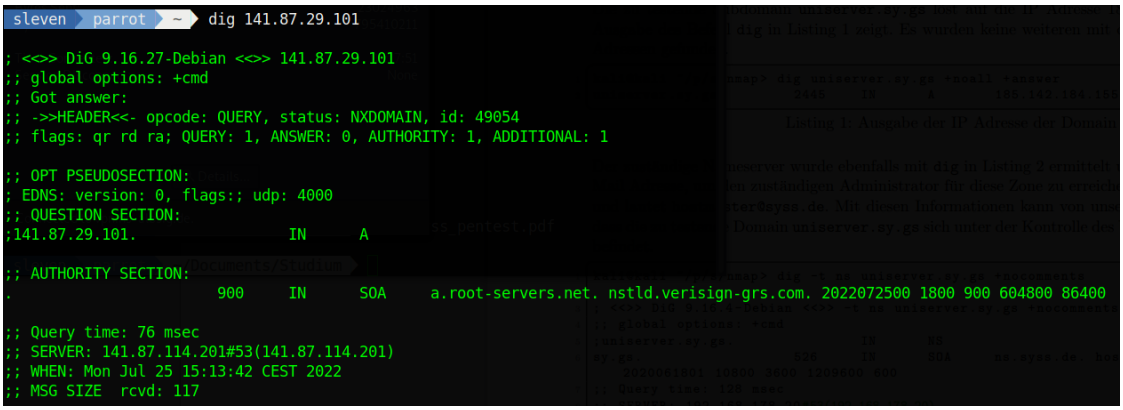
Die CCU3 ist ein Raspberry Pi 3b 2015. Die Hardware ist leicht zugänglich, und nur mit ein paar Schrauben gesichert. An den Raspberry Pi ist ein Custom Board angebracht, an dem sich eine Antenne befindet, welche den Zweck erfüllt, mit dem WLAN zu kommunizieren. Durch das einfache Öffnen des Gehäuses ist es möglich an die Speicherkarte zu gelangen und diese austauschen. Dadurch kann beliebige Schadware auf das System aufgespielt werden. Dies ist jedoch nur möglich, wenn direkter Zugriff zu dem Gerät besteht. Und ist abhängig vom jeweiligen Szenario. Im Falle einer Wohnungsvermietung könnte dies zu einer realistischen Gefahr werden.

7 Reconnaissance

Da die Anwendung über das Heimnetzwerk gehostet wird, ist keine generellen Domänen bzw. Plattformzuordnung möglich. Je nach eigener Konfiguration kann diese verschieden ausfallen.

In dem Testszenario wird die Anwendung über das Netzwerk der Hochschule Albstadt-Sigmaringen gehostet.

Einsehung mit dig:



Hierbei sehen wir die Autoritativer-name-server und den root Server. Diese sind allerdings bei jedem Benutzer unterschiedlich.

Der root Nameserver weist folgende dig Ergebnisse auf. Auch diese sind ausschließlich auf das Testsetup bezogen.

7.1 Fingerprinting

Einsehung der HTTP Header mit curl:

```
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
```

Hierbei fehlen einige wichtige HTTP Security Header.

7.2 Content Security Policy (csp):

Über die csp lässt sich detailliert steuern, ob die Verwendung von verschiedensten Datentypen auf einer Seite erlaubt ist und falls ja, aus welcher Quelle die Daten stammen müssen, damit sie als vertrauenswürdig gelten und somit ausgeführt werden. Dies kann verhindern das über Javascript Schadcode nachgeladen werden kann.

Empfohlene Konfiguration:

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

7.3 Strict-Transport-Security:

Da in der Standart-konfiguration die Webanwendung über HTTP läuft, ist dieser header nicht sinnvoll einsetzbar. Falls aber wie empfohlen auf HTTPS umgestellt wird, sollte dieser entsprechend verwendet werden.

Hierbei wird festgelegt das die gerade aufgerufene Seite für einen frei definierbaren Zeitraum (sinnvolle Werte liegen bei mindestens 6 Monaten) ausschließlich per HTTPS aufgerufen werden darf. HTTP-Verbindungen werden dann automatisch in HTTPS-Aufrufe umgewandelt.

Empfohlene Konfiguration:

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

7.4 Feature-Policy/Permission-Policy:

Dieser erlaubt es, die Nutzung bestimmter Funktionen, die für die Sicherheit oder den Datenschutz des Nutzers relevant sind, auf der Seite grundsätzliche zu verbieten. Zu diesen Funktionen gehören z.B. die Aktivierung von Webcam oder Mikrofon, der Abruf des Standorts, die Nutzung der Vibrationsfunktion oder die Aktivierung der ebenfalls noch relativ neuen Payment-API, die z.B. bei ApplePay Verwendung findet.

Über diesen Header kann man somit Schadcode unterdrücken, der es insbesondere auf Nutzer-Daten abgesehen hat.

Empfohlene Konfiguration:

Setze alle nicht benötigten features auf 'None'.

- **`Permissions-Policy: camera, document-write, geolocation=(none)`**

7.5 Portscan

Portscan mit Nmap:

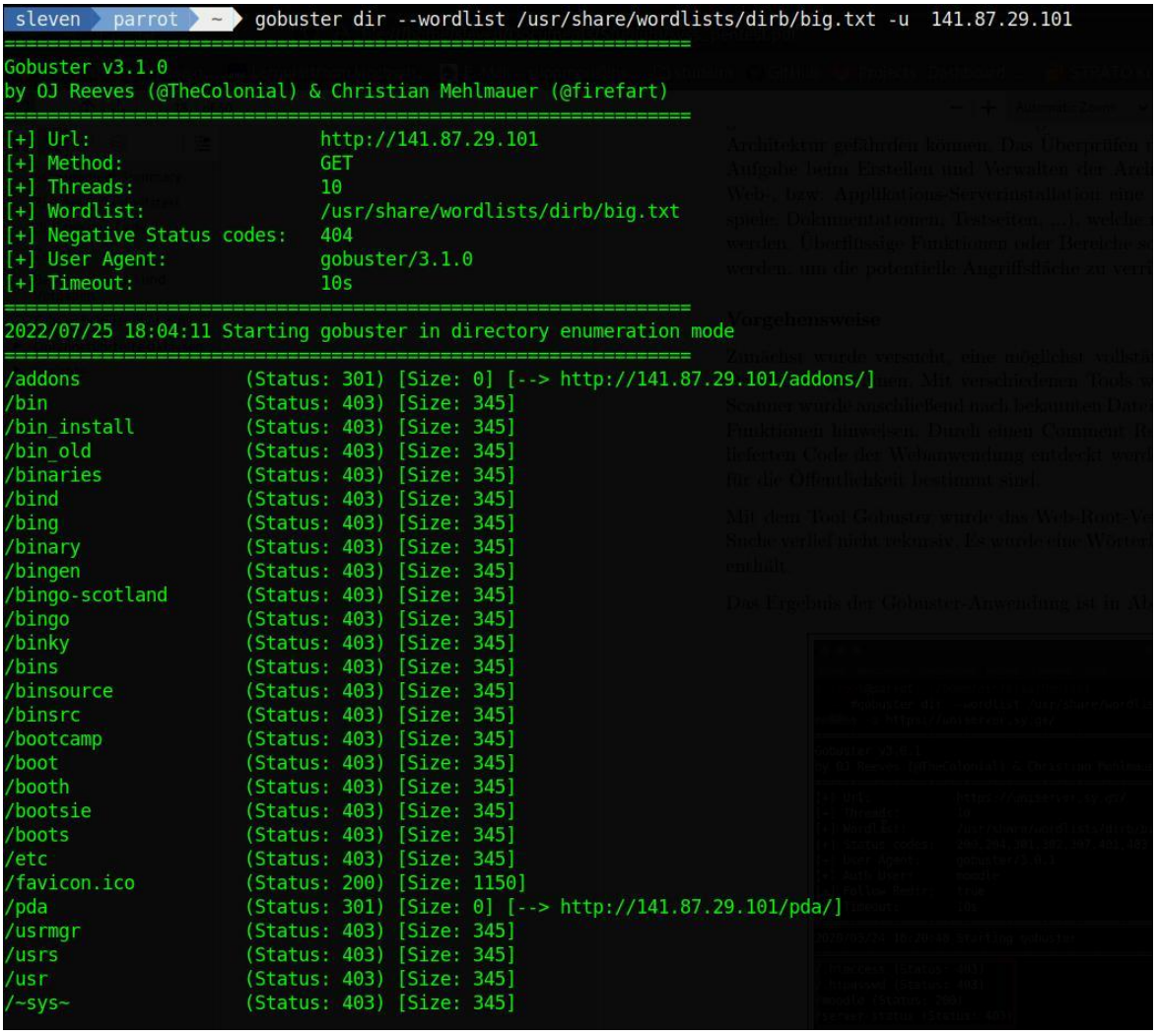
```
sleven  parrot  ~  nmap -sC -sV 141.87.29.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 15:12 CEST
Nmap scan report for 141.87.29.101
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.8 (protocol 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
```

Es ist zu vermuten das eine Firewall auf dem Gerät eingesetzt wird, da die Ports als gefiltert und nicht geschlossen angezeigt werden. Es wird empfohlen die Anwendung ausschließlich über HTTPS und Port 443 laufen zu lassen.

8 Plattform Konfiguration

Hierbei wurde die Ordnerstruktur der Webanwendung bzw. Des Web-Root Verzeichnisses untersucht. Bei falscher Konfiguration können sensitive Information einsehbar werden.

Anhand des tools gobuster wird die Ordnerstruktur sichtbar.



Die gefundenen Ressourcen wurden nun einzeln geprüft. Dabei wurden mehrere Schwachstellen ausfindig gemacht.

Anhand des Pentesting Tools OWASP ZAP wurden die Schwachstellen erneut gescannt und bestätigt.

8.1 Vulnerable JS Bibliothek

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

Die jquery Version 3.4.1 ist verwundbar für Ausführung nicht vertraulichem Programmcode. Die Schwachstelle ist in der CVE gelistet.

- CVE-2020-11023
- CVE-2020-11022

Empfehlung:

- Upgrade auf die neuste Version von jquery.

8.2 Fehlende Anti-CSRF Tokens in der Login-form

- http://141.87.29.101/login.htm
- http://141.87.29.101/login.htm?error=1

Über ein Cross-site request forgery Angriff ist es möglich die Same origin policy zu umgehen. Damit können Angreifer mit weiteren Webseiten Kommunizieren und somit potentiell schädliche Nutzeraktionen durchführen.

Empfehlung:

- Verwendung eines anti-CSRF Paketes wie der OWASP CSRFGuard.

  https://owasp.org/www-project-csrfguard/

8.3 Information Disclosure

Hierbei werden zugängliche Informationen wie der HTML/CSS Code, auf sensitive Informationen überprüft.

Mehrere Dateien weisen ein zu offenes Naming auf. Dies könnte Angreifer helfen Schwachstellen ausfindig zu machen bzw. an sensitive Informationen zu gelangen.

Beispielhaft die Datei https://141.87.29.101/pages/index.htm

```
UserButtonClick = function(fullName, name)
{
  $("UserNameShow").value = fullName;
  $("Password").value = "";
  $("Password").focus();
}

FormSubmit = function ()
{
  var tmp = $("UserNameShow").value;
  $("UserName").value = tmp.replace(' ','');
  document.getElementById( 'gwlogin' ).submit();
}

PasswordKeyUp = function(e)
{
  var keycode;
  if (window.event) keycode = window.event.keyCode;
  else if (e) keycode = e.which;
  else return;

  if (keycode == 13)
  { // ENTER
    FormSubmit();
```

Empfehlung:

- Anpassung aller Kommentare und Variablen Benennungen, sodass diese keine Informationen über Funktionalität aufweisen

8.4 Weitere betroffene Dateien

https://141.87.29.101/webui/js/common/viewmodels.js

https://141.87.29.101/webui/js/extern/excanvas.js

https://141.87.29.101/webui/js/extern/excanvas.js

https://141.87.29.101/webui/js/extern/jqplot.barRenderer.min.js

https://141.87.29.101/webui/js/extern/jqplot.canvasAxisTickRenderer.min.js

https://141.87.29.101/webui/js/extern/jqplot.canvasTextRenderer.min.js

https://141.87.29.101/webui/js/extern/jqplot.categoryAxisRenderer.min.js

https://141.87.29.101/webui/js/extern/jqplot.cursor.js

https://141.87.29.101/webui/js/extern/jqplot.cursor.js

https://141.87.29.101/webui/js/extern/jqplot.cursor.js

https://141.87.29.101/webui/js/extern/jqplot.markerRenderer.js

8.5 Session ID Rewrite

Bei Login wird eine Session ID angelegt. Diese ist in der URL abgreifbar. Gelangt man an die Session ID, wird man zu dem angemeldeten Nutzer mit seinen jeweiligen Rechten. Dies gilt auch für Admin Nutzer. Zudem ist die Session ID nach Inaktivität des Fensters 300 Sekunden lang gültig.

Die Session ID in der URL.

Die Session ID kann anhand des cross-site referer header offengelegt werden. Des Weiteren kann sie in Server Logs oder im Browser Verlauf gespeichert und abgerufen werden

Empfehlung:

- Session ID in ein einem Cookie speichern. Oder eine Kombination von Cookie Speicher und URL rewrite verwenden.
- Gültigkeit der Session ID nach Inaktivität auf 180 Sekunden reduzieren

9 Berichte

9.1 Brute Force

Um die CCU3 Brute Forcen zu können muss man zuerst Zugriff auf das lokale Netzwerk erlangen. Dies kann auch mithilfe einer Brute Force Attacke geschehen, indem man das WLAN-Passwort des Opfers Brute Forced. Brute Forcen ist eine Methode, mit der man durch Ausprobieren des Passwortes versucht, Zugriff auf ein Gerät oder andere Dinge zu erlangen. Dabei kann in der Brute Force Attacke eine Bibliothek verwendet werden. In dieser Bibliothek befinden sich meistens die am häufigsten genutzten Passwörter, wie zum Beispiel “Passwort123”. Die CCU3 zu Brute Forcen ist, wenn man Zugriff auf das lokale Netzwerk erlangt, hat gut möglich. Den Account, den der Angreifer ins Visier nehmen wird, ist der Admin Account, welchen der Techniker anlegt. Dieser besitzt nämlich alle Rechte des CCU3. Zudem wird das Passwort nie geändert, da der Techniker das Gerät nie wieder benutzen wird. Da die CCU3 keinen Cooldown hat, also wie viele Passwörter ausprobiert werden dürfen, bevor man eine zeitliche Sperre erhält, bevor man weitere Passwörter ausprobieren kann. Und zudem keine Benachrichtigung an dem Benutzer geschickt wird, falls ein Passwort zu oft falsch eingegeben wurde, kann der Angreifer so lang Passwörter ausprobieren bis er Zugriff auf den Admin Account erlangt. Um dies nun zu verhindern, sollte das Passwort, dass der Techniker für den Admin Account einstellt, kein Standartpasswort sein, sondern sollte am besten von einem Zufallsgenerator erstellt werden. Auch sollte nach zehnmaliger Falscheingabe des Passwortes ein Cooldown von einer Minute veranschlagt werden. Somit kann der Angreifer nicht unendlich viele Passwörter ausprobieren, bis er den Zugriff erlangt hat. Zudem sollte dieser Cooldown immer weiter steigen. Also wenn er das Passwort nochmal zehnmal falsch eingibt, ist der Cooldown dann 2 Minuten. Auch sollte der Besitzer des Homematic Geräts informiert werden, dass das Passwort eines Accounts zu oft falsch eingegeben wurde, sodass dieser selbst Vorsichtsmaßnahmen treffen kann, wenn sein Gerät eine Brute Force Attacke erleidet.

9.2 Skripte Hochladen

Die Funktion der CCU3 Skripte hochzuladen, um seinem Gerät neue Funktion anzulernen, beinhaltet eine große Gefahr sich dabei Schadsoftware auf sein Gerät hochzuladen. Die Skripte, die auf die CCU3 hochgeladen werden dürfen, können zwar nur ein paar Befehle besitzen, die von EQ-3 vorgegeben werden, jedoch kann ein Angreifer diese auch zu Schadsoftware umwandeln. Der Angreifer muss dabei nur ein Skript generieren und es auf ein Forum stellen, und warten bis es dann jemand auf sein Gerät hochlädt. Danach hat er dann die volle Kontrolle über das Smart Home seines Opfers. Jedoch ist die Risikostufe auf blau, da es für einen Angreifer einen sehr hohen Aufwand mit sich bringt ein solches Skript zu erstellen. Ebenso kann man sich sehr leicht vor dieser Art von Angriffen schützen, indem man keine Skripte aus Foren downloadet. Auch könnten die Skripte, bevor sie auf einem Forum hochgeladen werden, kontrolliert werden, ob dies Schadsoftware enthalten.

9.3 Software Update

9.3.1 Ablauf Softwareupdate

Die Softwareupdates werden von der CCU3 nicht automatisch durchgeführt. Unterhalb der Zeile mit der aktuellen Softwareversion (Firmware Version) erscheint eine neue Zeile, in der die verfügbaren Updates angezeigt werden. Diese Zeile erscheint aber nur wenn tatsächlich ein Update verfügbar ist, dabei spielt es aber keine Rolle, ob es sich um ein Softwareupdate der CCU3 selbst oder um ein Softwareupdate eines angeschlossenen Gerätes handelt. Sollten mehr als ein Softwareupdate verfügbar sein wird dies dargestellt, indem am Ende der erschienenen Zeile eine Zahl entsprechend der Anzahl der verfügbaren Updates in Klammer steht.

Bevor ein Update durchgeführt wird, muss immer ein Backup erstellt werden damit, falls es zu einem Absturz oder Abbruch kommt, keine Daten verloren gehen. Die Backup Option kann in den Einstellungen unter Sicherheit gefunden werden. Dieses Backup ist eine .sbk Datei und kann bei Bedarf einfach auf den Homematic CCU3 aufgespielt werden.

Das Update wird entweder über die Zentralenwartung oder direkt über einen Klick auf die oben genannte Updatezeile heruntergeladen. Das Update wird dabei nicht direkt auf den Homematic CCU3 geladen, sondern wird z.B. zunächst auf dem Gerät, das das Update über die Weboberfläche herunterlädt, gespeichert. Anschließend muss man das Softwareupdate in der Zentralenwartung auswählen. Nachdem dies passiert, ist kann die Software auf die CCU3 geladen werden. Dies dauerte bei uns etwa 5 Minuten. Dies liegt aber auch daran das an unserem Homematic keine weiteren Geräte angeschlossen sind. Der Homematic CCU3 verfügt über einen Duty Cycle dieser gibt an, wie sehr das Gerät ausgelastet ist. Wenn ein Update durchgeführt oder hochgeladen wird kann die Auslastung des Duty Cycle schnell steigen, wenn der Duty Cycle ausgelastet ist, dauert das Update entsprechend länger. Nachdem das Update auf den Homematic hochgeladen wurde, muss dieses noch installiert werden, auch hier hängt die Dauer von der Auslastung des Duty Cycle ab.

9.3.2 Probleme beim Softwareupdate

Da bei einer hohen Auslastung im Duty Cycle ein Update mehrere Stunden dauern kann, wird in diversen CCU3 Foren empfohlen die Updates dann auszuführen, wenn man nicht zuhause ist. Sie schlagen zum Beispiel vor die CCU3 dann zu Updaten, wenn man in den Urlaub fährt.

Dadurch das die Softwareupdates händisch installiert werden müssen ergeben sich neue Probleme. Den damit kann es sein das Geräte mit einer veralteten Software und den entsprechenden Sicherheitslücken trotzdem in Betrieb sind.

Manchmal verzichten die Nutzer aber auch freiwillig auf ein Update, den in der Vergangenheit war es bereits so, dass manche Updates neben den üblichen Verbesserungen auch Nachteile für den User hatten, indem dann zum Beispiel angeschlossene Geräte nicht mehr richtig funktioniert haben. Deshalb verzichten auch einige Nutzer darauf das Gerät zu updaten, wenn es erst einmal in Betrieb ist. Die Gefahr, die durch eine veraltete Software entsteht, wird dabei oft unterschätzt. Deshalb ist es wichtig das, wenn ein Techniker vor Ort ist alle Updates durchgeführt werden.

Wenn die Software des Homematic CCU3 auf dem aktuellen Stand ist, dann gibt es keine bekannten Schwachstellen. Wichtig ist zu überprüfen das das Gerät auf jeden Fall mit einer Softwareversion von mindestens 3.59.6 betrieben wird, sollte dem nicht so sein gibt es eine Schwachstelle die laut NIST mit

einem Score von 10 kritisch ist. Das Firmwareupdate 3.59.6 wurde am 29.06.2021 von EQ-3 bereitgestellt. Damit sind Geräte, die vor diesem Datum produziert wurden und jetzt erst ausgeliefert werden eventuell noch von der Sicherheitslücke betroffen.

Ein weiteres Problem ist, Updates können nur vom Admin durchgeführt werden, dadurch das nur der Techniker einen Admin Zugang besitzt kann auch entsprechend nur er die Updates durchführen. Sollte eine neue kritische Schwachstelle gefunden werden kann es sein das eventuell nicht sofort reagiert werden kann. Damit kann es aber auch sein das sehr viele Geräte zur gleichen Zeit geupdatet werden müssen, dies kann dann dazu führen, bei einer begrenzten Anzahl an Technikern und der Dauer eines Updates mit hoher Auslastung des Duty Cycles, kann es dann zu längeren Wartezeiten und einem gestiegenen Risiko für die Kunden kommen.

9.4 Remote Code Execution

Grundsätzlich geht von einer Remote Code Execution für die Homematic CCU3 zurzeit keine Gefahr mehr aus. Aktuell gibt es keine bekannten Sicherheitslücken, die eine RCE (Remote Code Execution) ermöglichen, dies gilt allerdings nur wenn das System über die aktuellen Sicherheitsupdates verfügt. Dabei ist auch hier das Firmwareupdate 3.59.6 vom 29.06.21 zu erwähnen den dort wurden die letzten bekannten Schwachstellen, die eine RCE ermöglichen gepatcht.

Allgemein lässt sich über die Vergangenheit sagen das für eine RCE zuerst eine SessionID abgefangen werden muss. Diese SessionID konnte z.B. im CVE-2019-9583 abgefangen werden, indem man verschiedene HTTP Request durchgeführt hat. Anschließend konnte aus dem Header der Response die SessionID ausgelesen werden.

Mit dieser SessionID konnte man sich dann einfach anmelden und Zugang auf die Weboberfläche bekommen, dieser Zugang konnte dann für RCE oder andere Angriffe ausgenutzt werden.

9.5 Replay Angriff auf Homematic Smart Home Systeme

Alle folgenden Szenarien setzen die Möglichkeit eines Replay Angriff voraus, (unabhängig ob Rolling Code oder nicht verwendet wird)

Szenario Vollvernetzung:

In diesem Szenario wird die CCU3 zur Steuerung von potentiell sicherheitsrelevanten Geräten verwendet, wie zum Beispiel Türschlössern oder Rollladensteuerungen.

Ein Replay Angriff kann hier verwendet werden, um die Türen oder Rollläden nach Bedarf zu öffnen oder schließen, außerdem ist auch Infrastruktur wie z.B. Heizungssteuerungen oder Stromverbraucher an steuerbaren Steckdosen betroffen.

Mittels eines SDR konnten wir von der Basisstation ausgehende Funksignale mit einer Frequenz von +- 868,3 MHz ermitteln, diese dienen der Kommunikation zwischen Basisstation und zusätzlichen Modulen wie z.B. der Relais Steckdose.

Das Funkprotokoll scheint eine Bestätigung des Signals zu beinhalten, da kurz nach einem an/aus Signal der Basisstation eine Antwort auf derselben Frequenz erfolgt.

Bei den meisten Systemen auf 433MHz oder 868MHz Basis wird immer dasselbe Signal für die Steuerung verwendet, aufgrund der zu geringen Auflösung unseres SDR´s ist dies aber in diesem Fall nicht eindeutig feststellbar.

Unter der Annahme, dass es in diesem Fall auch nur ein umcodiertes bzw. unverschlüsseltes Signal ist, wäre ein Replay Angriff auf dieses System denkbar, hierzu kann man ein SDR verwenden, um ein Steuersignal aufzuzeichnen und dieses dann abzuspielen um ein An oder Abschalten der Gerätschaft zu einem späteren Zeitpunkt zu erreichen.

Mit dieser Methode kann man dann alle mit der Basisstation verbundenen Geräte ein oder ausschalten, darunter beispielsweise Lichter, Heizungssteuerungen, Sprinkleranlagen oder noch Kritischere Systeme.

9.6 Hardware Angriffe

Mittels eines "USB-Killers" lässt sich in Sekundenbruchteilen ein dauerhafter DOS Angriff auf die Basisstation ausführen, durchgeführt durch jede Person
die ein paar Sekunden Zugriff auf die Station erhält.
Der USB-Killer erzeugt aus den 5v die am USB-Port anliegen einen Hochspannungspuls, der die ungeschützte Elektronik im Raspberry Pi zerstört
und dadurch entweder einen dauerhaften Kurzschluss auslöst oder den Prozessor unbrauchbar macht.

Die SD-Karte im inneren des Gehäuses enthält die gesamte unverschlüsselte Software der CCU3, im Falle eines Physischen Zugriffs auf die CCU3 durch einen Angreifer wie z.B. in einem Ferienhaus könnte dieser von dieser die Passwort Hashes der Admin Accounts auslesen oder Veränderungen in der Weboberfläche vornehmen.

Die Hashwerte der Passwörter sind nicht gesalted o.ä. und verwenden SHA-512. Mittels dieser Hash Werte kann man dann versuchen das Admin Passwort zu cracken (Rainbowtable oder Brute Force)

9.7 SSH Zugang:

Die Anwendung besitzt einen SSH Zugang, der im Auslieferungszustand nicht aktiviert ist. Der Zugang kann nur mithilfe von Admin Rechten aktiviert und konfiguriert werden. Über diesen gelangt man auf das File System der Weboberfläche. Ist man im Besitz der SSH Zugangsdaten können jegliche Daten der Anwendung mitgelesen und verändert werden. Auch kann die Benutzeroberfläche an sich manipuliert werden. So könnte Schadcode wie ein Keylogger installiert werden. Da der Handwerker als einziger Admin Rechte besitzt, kann der Benutzer dies nicht Prüfen oder sichern.

Empfehlung:

- Betreiber der CCU sollten Admin Rechte erlangen und sofort nach Einrichtung des Handwerkers die SSH Zugänge prüfen bzw. mit neuen Anmeldedaten versehen.

10. Quellen

https://owasp.org/

https://www.eq-3.com/products/homematic/detail/smart-home-central-control-unit-ccu3.html

https://homematic-ip.com/de/produkt/smart-home-zentrale-ccu3

https://github.com/psytester/psytester.github.io/blob/master/_posts/hacking_and_pentests/CVEs/2019-03-27-CVE-2019-9583.md