homematic IP

eQ-3 PRESSEINFORMATION

Smart-Home-Sicherheit auch bei unsicheren Heim-Netzen und Port Forwarding

eQ-3 schließt Sicherheitslücken in der CCU

Leer, 18. März 2019 – eQ-3, der Europamarktführer im Smart-Home-Bereich[1], hat heute neue Updates seiner Smart Home Zentrale für Profis, der CCU3 und der CCU2, veröffentlicht. Damit wurden mehrere potentielle Sicherheitslücken geschlossen. In bestimmten Situationen war es möglich, dass Unberechtigte sich Zugang zur CCU verschaffen konnten. Zwingende Voraussetzung ist in diesen Fällen, dass entweder das sogenannte Port Forwarding für den Remote Zugriff verwendet wird oder dass das Heim-LAN insgesamt unsicher ist und Fremde somit Zugriff haben. eQ-3 ist es wichtig, dass auch solche Lücken geschlossen werden, die für die meisten Installationen keine Rolle spielen.

Port Forwarding wurde in den „frühen" Tagen der Internetnutzung verwendet, um von überall Zugriff auf Geräte im Heim-LAN zu bekommen, und war insbesondere bei LAN-Kameras viele Jahre populär. Port Forwarding erlaubt es letztlich jedem System im Internet, ohne Authentisierung auf das betroffene Gerät zuzugreifen, um dort nach Sicherheitslücken zu suchen. Natürlich gibt es inzwischen Alternativen zu Port Forwarding, bei denen dies nicht mehr möglich ist. eQ-3 warnt bereits seit mehreren Jahren vor dem Einsatz von Port Forwarding. Seit 2017 ist es bei der Installation der CCU oder einer neuen Software-Version sogar notwendig, dass der Nutzer diese Warnung explizit bestätigt. eQ-3 empfiehlt seit vielen Jahren, dass Nutzer statt Port Forwarding andere Techniken wie VPN-Verbindungen – z.B. mit Fritz!Fernzugang – oder die Serverlösung „CloudMatic Connect" von der Firma EASY SmartHome verwenden.

Die Firma Open Source Security („OS-S") hat eQ-3 in den letzten Wochen vor mehreren Sicherheitslücken gewarnt, die bei der CCU beim Zugriff aus dem LAN oder via Port Forwarding bestehen. Informationen über die gleichen potentiellen Sicher-

[1] Laut Berg Insight ist eQ-3 der europäische Marktführer für Smart Home in Bezug auf die installierte Basis von Whole-Home-Lösungen; d.h. eQ-3 hat eine installierte Basis, die größer ist, als die der drei nächsten folgenden Hersteller plus aller KNX-Lösungen im Heimbereich.

heitslücken und deren Behebung wurden in den letzten Wochen mit dem BSI-CERT ausgetauscht. Obwohl nur Nutzer betroffen sind, die gegen Sicherheitshinweise von eQ-3 verstoßen oder seit mehreren Jahren keine Sicherheitsupdates installiert haben, gibt eQ-3 solchen Fällen hohe Priorität und behebt entsprechende Sicherheitslücken schnellstmöglich nach Bekanntwerden in neuen Software-Versionen und Hotfixes.

Homematic IP ist als Smart-Home-Lösung mit dem HAP, der Cloud und den Smartphone Apps von den potentiellen Sicherheitslücken schon daher nicht betroffen, weil der HAP kein Linux, sondern ein Echtzeitbetriebssystem einsetzt. Entsprechend ist auch die erfolgte Zertifizierung der Protokoll-, IT- und Datensicherheit von Homematic IP durch den VDE nicht berührt.

Im Anhang zu dieser Presseinformation und im Change Log zu allen neuen Software Releases findet sich jeweils eine Beschreibung aller Erweiterungen, Änderungen und behobener potentieller Sicherheitslücken. Diese können unter diesem Link heruntergeladen werden: https://www.eq-3.de/service/downloads.html.

Über eQ-3:

eQ-3 zählt zu den Innovations- und Technologieführern im Smart-Home-Markt, das heißt insbesondere im Bereich der Home-Control-Lösungen. 2018 wurde eQ-3 vom renommierten Marktforscher Berg Insight zum vierten Mal in Folge zum Marktführer in Europa gekürt. eQ-3 hat mit eigenen Marken und OEM-Produkten einen Anteil von 35 % der installierten Basis aller Whole-Home-Systeme in Europa. Mit mehr als 200 Produkttypen verfügt eQ-3 über das industrieweit breiteste Smart-Home-Angebotsportfolio und hat mehr als 30 Millionen Funklösungen in mehr als 1,7 Millionen Haushalte vermarktet. Design und Produktentwicklung erfolgen mit mehr als 90 Entwicklern in der Firmenzentrale in Leer. Produziert wird im eigenen Werk in Zhuhai, Südchina, das mit Bestnoten des BSCI zur Corporate Social Responsibility und den Zertifizierungen ISO 14001 und ISO 9001 für das Umwelt- und Qualitätsmanagement überzeugt. 2007 wurde die eQ-3 AG aus der seit nunmehr 40 Jahren bestehenden ELV ausgegründet. Die Unternehmensgruppe befindet sich zu 100 % in Besitz des Gründers und Vorstandsvorsitzenden, Prof. Heinz-G. Redeker.

Weitere Informationen: www.homematic-ip.com, www.eQ-3.de

Pressekontakt:
eQ-3 AG
+49 (491) 6008 – 627
presse@eq-3.de
Maiburger Straße 29
D-26789 Leer

PR-Agentur:
Benjamin Kolthoff
P.U.N.K.T. Gesellschaft für Public Relations mbH
+49 (40) 85 37 60 - 29
bkolthoff@punkt-pr.de
Völckersstraße 44
D-22765 Hamburg

homematic IP

eQ-3 PRESSEINFORMATION

Anhang:

Die heute veröffentlichten Software Versionen für die CCU2 und CCU3 beheben folgende Fehler:

- **Buffer Overflow im ReGa Web Server**
  Im ReGa Web Server gibt es eine Pufferüberlauf- / Buffer Overflow Schwachstelle. Bei dieser können in einen Datenbereich (Array) mit fester Größe im Stack Daten beliebiger Länge geschrieben. Durch „bösartiges“ Schreiben von Daten, ist es prinzipiell möglich, die Rücksprungadresse im Stack zu Überschreiben und den Rücksprung in den Bereich der geschriebenen Daten zu lenken. Hierdurch könnte Schadcode ausgeführt werden. Aktuell ist jedoch kein Exploit bekannt, der dies für einen Angriff auf die CCU ausnutzt. Der Webserver-Prozess kann aber zum Absturz gebracht werden. Die Schwachstelle des Pufferüberlauf- / Buffer Overflow wurde geschlossen. Damit kann hier kein Schadcode mehr eingeschleust werden.

- **Schreiben beliebiger Daten**
  Unter bestimmten Umständen war das Schreiben beliebiger Daten möglich. Hier wurde ein Fehler in einem Script für die Administration behoben.

- **Remote Execution**
  Unter bestimmten Umständen war eine Remote Execution von Tcl Scripten über das Heim-LAN möglich.
  Hier wurde ein Fehler in einem Script für die Administration behoben.

- **Unberechtigtes Login durch Manipulation mit der SessionID**
  Durch das Aufrufen der WebUI wird bereits vor dem Login eines Benutzers eine Sitzung / SessionID erzeugt. Diese kann für weiterführende Angriffe missbraucht werden. In der Problembehebung wird die Erzeugung einer Sitzung / SessionID ohne vorherigen Login verhindert

- **Authentication Bypass durch User „RemoteAPI”**
  Über einen in der Logikschicht der CCU existierenden internen Benutzer „RemoteAPI“ kann eine gültige Sitzung / SessionID erzeugt werden, die die Basis für weiterführende Angriffsszenarien darstellt. Die Erzeugung einer Session für den internen Benutzer wird jetzt unterbunden.

- **Fehler im Session Handling**
  Beim Ausloggen / Abmelden eines Benutzers aus der CCU WebUI wird die Sitzung / SessionID durch ReGa in bestimmten Situationen nicht sofort invalidiert. Dadurch kann die SessionID unter diesen Umständen zeitweilig für einige Aufrufe weiterverwendet werden. Die SessionID wird jetzt sofort beim Abmelden eines Benutzers invalidiert. Eine weitere Verwendung ist damit nicht mehr möglich.

Risiko:

Folgende Angriffsmöglichkeiten bestanden zuvor bei diesen Fehlern

- aus dem Internet,wenn Port Forwarding eingerichtet war
- aus dem LAN, wenn unsichere Systeme Zugang zum Heim-LAN haben