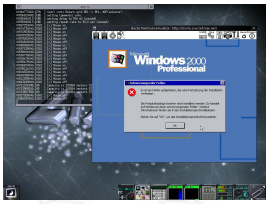

Sicherheitslücken bedrohen beliebte Smart-Home-Geräte - Laut ESET-Forschern können Angreifer Schaltzentralen des Smart Homes übernehmen

Forscher des IT-Sicherheitsherstellers ESET haben in drei beliebten Smart-Home-Kontrollzentralen und Geräten gravierende Sicherheitslücken entdeckt. Zu den betroffenen Geräten zählen die in Deutschland an Privatanwender und kleinen Unternehmen viel verkauften HomeMatic Central Control Unit (CCU2), Fibaro Home Center Lite und eLAN-RF-003. Über die Schwachstellen können sich Angreifer die Kontrolle über die Geräte verschaffen und dadurch Man-in-the-middle-Angriffe durchführen, Opfer belauschen, sensible Daten stehlen, Hintertüren öffnen oder Root-Zugriff auf einige der Geräte erlangen. Im schlimmsten Fall schaffen es Hacker, über die Schaltzentralen die umfassende Kontrolle über das jeweilige Smart Home zu erlangen.
ESET hatte bereits 2018 die betroffenen Hersteller informiert, die umgehend mit Sicherheits-Updates reagiert haben. Da Updates händisch bestätigt werden müssen, ist von einer großen Anzahl ungepatchter Geräte auszugehen, die immer noch über die bekannten Schwachstellen verfügen. ESET empfiehlt Nutzern eindringlich, die neuen Programmversionen zeitnah einzuspielen. Die detaillierte Analyse befindet sich im ESET-Securityblog.

"Sicherheitslücken in IoT-Geräten sind ein weit verbreitetes und vielfach noch immer unterschätztes Problem. Mängel in den Einstellungen sowie die fehlende Verschlüsselung oder Authentifizierung treten nicht nur bei billigen Low-End-Geräten auf. Leider krankt auch High-End-Hardware sehr oft daran", sagt ESET-Security-and-Awareness-Spezialist Ondrej Kubovic.

Homematic CCU2

Die zentrale Steuereinheit des Smart-Home-Systems von eQ-3 zeigte während des ESET-Tests einen schwerwiegenden Sicherheitsmangel. Angreifer hätten als Root-Benutzer eine nicht authentifizierte Remote-Code-Ausführung (RCE) durchführen können. Mit entsprechenden Shell-Befehlen wäre der volle Zugriff auf die Schaltzentrale und auch auf angeschlossene Peripheriegeräte möglich gewesen. Da eQ-3 mit seinen Eigenmarken und OEM-Produkten einen Anteil von 40 Prozent installierten Basis aller "Whole-Home-Systeme" in Europa besitzt, hat diese Sicherheitslücke eine enorme Relevanz.

RF-Box eLAN-RF-003

Auch die Zentraleinheit RF-Box eLAN-RF-003 wies in der ESET-Analyse deutliche Schwachstellen auf. Die Sicherheitsexperten testeten das Gerät zusammen mit zwei Peripheriegeräten desselben Herstellers: einer drahtlos dimmbaren LED-Birne und einer dimmbaren Fassung. Eine unzureichende Befehlsauthentifizierung hätte es ermöglicht, dass Hacker alle Befehle ohne Anmeldung hätten ausführen können. Zudem zeigte sich, dass die Funkkommunikation mit Peripheriegeräten anfällig war für spezielle Netzwerkattacken, sogenannte "Record and Replay"-Angriffe.

Fibaro Home Center Lite

Der Home-Automation-Controller soll eigentlich die Peripheriegeräte im Smart Home steuern. Zahlreiche gravierende Schwachstellen hätten zum Super-GAU führen können. Angreifer wären in der Lage gewesen, eine SSH-Hintertür zu erstellen, Schadcode auszuführen und letztlich die volle Kontrolle über das Zielgerät zu erlangen.