Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan Bund ISB
Informatiksicherheit SEC

Hans Oppliger

04. Dezember 2019

Technologiebetrachtung

Angreifbare Logitech Geräte

1 Einleitung

In Ausgabe 8/19 berichtete die Computer Zeitschrift c't im Rahmen der Artikelreihe «Hacking Gadgets» über einen Angriff auf die weit verbreiteten PowerPoint-Fernbedienungen Logitech Presenter, welcher schwerwiegende Folgen haben kann. Während der USB-Empfänger des Presenters mit dem Rechner verbunden ist, kann ein Angreifer in Funkreichweite mit Hilfe eines speziell präparierten Funkmoduls beliebige Befehle auf dem System ausführen. Auf diese Weise können böswillige Personen nicht nur Präsentationen vor grossem Publikum sabotieren, sondern auch Schadcode einschleusen.

Die USB-Empfänger akzeptieren nicht nur die Steuerbefehle für PowerPoint ("Bild auf" und "Bild ab"), sondern auch beliebige Tastatureingaben. Und wer Tastenbefehle eingeben kann, der hat die Hoheit über ein System: Ein Angreifer würde typischerweise unter Windows mit Windows+R den Ausführen-Dialog öffnen und anschliessend die PowerShell starten. Damit lädt der Angreifer Schadcode nach und lässt diesen ausführen. Welches Betriebssystem auf dem Rechner läuft, spielt übrigens keine Rolle – der Schadcode muss lediglich dazu passen.

Wie Logitech erklärte, sind die Presenter-Modelle R400, R700 und R800 durch die Schwachstelle angreifbar. Damit schaffte das Unternehmen erstmals Klarheit über ein seit mindestens drei Jahren bekanntes Sicherheitsproblem. Die bisher verfügbaren Informationen über die Anfälligkeit stammten nämlich nicht von Logitech, sondern von unabhängigen Security-Experten der SySS GmbH.

So dokumentierte der SySS-Forscher Matthias Deeg die Lücke im Modell R400 bereits im Jahr 2016 und vor kurzem konnte er das Problem auch bei dem Modell R700 nachweisen [1]. Darüber, dass auch die Wireless Presenter des Typs R800 betroffen sind, informierte Logitech erst auf Nachfragen der Presse.

Mittlerweile tauscht Logitech verwundbare USB-Empfänger der Logitech-Presenter-Reihe aus. Zudem räumt das Unternehmen ein, dass viel mehr Geräte von gleich mehreren gefährlichen Sicherheitslücken im Funkprotokoll betroffen sind als bisher bekannt.

So wurden, wiederum von externen Security-Experten, gleich mehrere Sicherheitslücken in kabellosen Tastaturen, Gaming-Produkten und Mäusen der Firma Logitech gefunden, die die proprietäre Unifying-Funktechnik einsetzen. Die Angriffsszenarien und die möglichen Auswirkungen sind die gleichen wie bei der Schwachstelle bei den Presenter-Modellen.

2 Welche Geräte sind genau betroffen?

Bei den Presenter-Modellen sind nach heutigem Stand nur die drei erwähnten Modelle R400, R700 und R800 von der ursprünglichen Schwachstelle betroffen. Allerdings sind diese sehr weit verbreitet – auch innerhalb der BVerw. Im Gegensatz zu den anderen Geräten gibt es dafür keine Firmware-Updates und die USB-Empfänger müssen beim Hersteller ausgetauscht werden [2].

Leider sind die Informationen von Logitech etwas verwirrlich. Auf den Supportseiten wird auf eine neue Firmware verwiesen, welche aber nicht durch den Benutzer installierbar ist. Vielmehr muss sich dieser an den Logitech Kundendienst wenden, um einen Ersatzempfänger mit der neuen Firmware zu erhalten. Selbst bei einer Neubeschaffung im Geschäft oder Onlinehandel muss noch damit gerechnet werden, einen USB-Empfänger mit anfälliger Firmware-Version zu erhalten.

Kommentare auf den Supportforen von Logitech lassen erahnen, dass die Schwierigkeiten diesbezüglich vielfältiger Art sind. So soll Logitech bis vor kurzem gar nicht in der Lage gewesen sein, diese Ersatzempfänger zu liefern und wenn man dann endlich das Teil erhalten hat, war es vielen Kunden offensichtlich nicht möglich dieses neu zu pairen. Dazu muss eine Software bei Logitech heruntergeladen werden, welche scheinbar nicht zuverlässig funktioniert. Auf unseren APS wäre diese Software wegen AppLocker nicht ausführbar oder müsste erst zugelassen werden.

Bei den anderen Geräten sind gemäss Logitech alle Tastaturen und Mäuse betroffen, welche die Unifying-Funktechnik einsetzen. Darüber hinaus sind kabellose Gaming-Produkte der Lightspeed-Serie, sowie die Logitech Presenter R500 und Spotlight für die jüngst bekannt gewordenen Schwachstellen anfällig. [3]

Die Unifying-Geräte erkennen Sie an einem orangefarbenen Logo mit Stern, das sich auf dem Eingabegerät selbst und auf dem USB-Empfänger befinden kann. Im Zweifel erfahren Sie über das Datenblatt, ob die Unifying-Technik zum Einsatz kommt. Logitech liefert seit 2009 kabellose Geräte mit Unifying-Empfängern aus. Die anfälligen Presenter und die Gaming-Produkte tragen kein solches Logo.

Der Angreifer würde in den meisten Fällen den USB-Empfänger attackieren. Welches Eingabegerät Sie daran betreiben, spielt keine tragende Rolle.

Die meisten Schwachstellen kann der Angreifer nur ausnutzen, wenn er zumindest kurzzeitig vor Ort ist und Zugriff auf den USB-Empfänger hat. Der Zugriff dauert nur wenige Sekunden und dürfte zum Beispiel in einem Großraumbüro nicht weiter auffallen [4]. Danach hat der Angreifer fortwährenden Zugriff auf den Rechner, unabhängig davon ob dieser mit einem Netzwerk verbunden ist. Manche der Lücken kann der Angreifer auch ohne physischen Kontakt zum USB-Empfänger ausnutzen.

Laut der Logitech-Supportseite [4] muss sich der Angreifer auf 10 Meter nähern. Unifying wird mit einer Reichweite von 10 Metern beworben, darauf sollte man sich aber nicht verlassen. Im Jahr 2016 erklärte das Forscherteam hinter dem "Mousejack"-Angriff, dass Logitechs drahtlose Eingabegeräte aus einer Distanz von maximal 100 Metern attackiert werden können. Die Forscher nutzten einen USB-Funkstick mit Sende- und Empfangsverstärker, wie er für ca. CHF 40 im freien Handel erhältlich ist.

Logitech hat im August 2019 Firmware Updates für die verschiedenen Unifying USB-Empfänger zur Verfügung gestellt [5] – weist allerdings selber darauf hin, dass nicht alle Schwachstellen gepatcht werden, um die Interoperabilität der Unifying-Geräte untereinander aufrecht erhalten zu können. Zum Patchen würde das Logitech

Firmware Update Tool SecureDFU verwendet, welches auf den APS der BVerw nicht genutzt oder installiert wird. Es ist also von vielen ungepatchten USB-Empfängern auszugehen, welche auch nicht ohne beträchtlichen Aufwand gepatcht werden können [6].

3 Einschätzung

Mit dem Bekanntwerden dieser Sicherheitslücken im Logitech Unifying-Funkprotokoll wurden die Risiken im Gebrauch von kabelloser Peripherie exemplarisch aufgezeigt. Selbst wenn man alle verfügbaren Updates installieren könnte, würden immer noch Restrisiken bestehen bleiben - weil Logitech nicht alle Schwachstellen korrigieren will, um die Rückwärtskompatibilität der Geräte nicht zu gefährden.

Dabei handelt es sich um gefährliche und einfach auszunutzende Schwachstellen.

Dem Benutzer bleibt lediglich sich auf diese Risiken einzustellen und sein Verhalten entsprechend anzupassen.

An erster Stelle müsste stehen auf den Gebrauch solcher kabellosen Peripherie möglichst zu verzichten – und falls doch notwendig Geräte einzusetzen, welche auf den Standard-Funkprotokollen wie WLAN oder Bluetooth aufsetzen. Auch damit kommt es hin und wieder zu Problemen, allerdings dürften diese durch die weite Verbreitung schneller publik und korrigiert werden.

Es gibt einzelne betroffene Logitech-Produkte, welche wahlweise über Unifying oder Bluetooth betrieben werden können. Sollte man ein solches Produkt besitzen, soll auf jeden Fall Bluetooth genutzt werden – da immer der Unifying-Funkempfänger der Angriffspunkt ist.

Will man solche Produkte weiter einsetzen, dann sollen die USB-Funkempfänger bei Nichtgebrauch immer abgezogen und mitgenommen werden. Das Gerät unbeaufsichtigt herumstehen zu lassen ist eine schlechte Idee – der Angreifer benötigt nur wenige Sekunden Zugriff auf einen solchen Empfänger, um ihn entsprechend zu manipulieren. Diejenigen Schwachstellen, welche zur Ausnutzung einen kurzen physischen Zugriff auf die Peripheriegeräte voraussetzen, wurden nicht gepatcht. Deshalb sollte diese Hardware auch nicht unkontrolliert ausgeliehen werden.

Wenigstens die zur Verfügung stehenden Patches sollten installiert werden. Die LE prüfen den Rollout des Firmware Update Tool von Logitech. Bei den von der ursprünglichen Schwachstelle betroffenen Presenter-Modellen müssen die USB-Empfänger ausgetauscht werden.

Bei Präsentationen vor grossem Publikum am besten nicht das eigene Arbeitsgerät, sondern ein Poolgerät verwenden, damit die eigenen Daten nicht gefährdet werden.

Letztlich muss auch gesagt werden, dass sich die genannten Risiken nicht auf Produkte der Firma Logitech beschränken. Auch andere Hersteller setzen auf proprietäre Funkprotokolle zur Anbindung von Peripheriegeräten - typischerweise erkennbar an einem mitgelieferten USB-Dongle. Bekannt sind z.B. auch Angriffe bzw. das Abhören der weit verbreiteten kabellosen Microsoft-Tastaturen [7].

4 Weiteres Vorgehen

Das BBL soll den Produktekatalog dahingehend anpassen, dass nur noch Peripheriegeräte bestellt werden können, welche entweder mittels Kabel, oder falls kabellos, über WLAN oder Bluetooth mit dem APS verbunden werden können.

Die ISBD sind besorgt, die vorliegenden Informationen in ihren Departementen zugänglich zu machen und die Benutzer aufzufordern, das Patchen oder den Austausch bei betroffenen Geräten zu initiieren. Den Endbenutzer direkt zu informieren ist wichtig, weil vermutlich auch viele privat beschaffte Geräte im Einsatz sind.

Die generellen Risiken beim Einsatz von kabellosen Peripheriegeräten soll in zukünftigen Sicherheitskampagnen weiter thematisiert werden.

Abkürzungen

SySS	SySS GmbH, Dienstleister im Bereich IT-Sicherheit
USB	Universal Serial Bus, Schnittstelle für Peripheriegeräte
APS	Arbeitsplatz System
BVerw	Bundesverwaltung
ISB	Informatiksteuerungsorgan des Bundes
z.B.	zum Beispiel

Referenzen

[1] Pentest Blog der Fa. SySS: SYSS-2016-74 und 75: Schwachstellen in kabellosen Präsentationsgeräten (Wireless Presenter): https://www.syss.de/pentest-blog/2016/syss-2016-74-und-75-schwachstellen-in-kabellosen-praesentations-geraeten-wireless-presenter/

[2] Logitech Update zu den Presentern R400, R700 und R800: https://support.logi.com/hc/en-us/community/posts/360033353213-Logitech-Update-zu-den-Presentern-R400-R700-und-R800

[3] Beispiel eines Angriffs auf eine kabellose Maus – ohne physischen Kontakt zum Empfänger (dieser Angriff dürfte nicht mehr funktionieren, falls Maus im August gepatcht wurde): https://www.youtube.com/watch?v=nZjpgT1KreY

[4] Beispiel eines Angriffs mit notwendigem, einmaligem Zugriff auf das Gerät: https://www.youtube.com/watch?v=MauTMsyphUE&feature=youtu.be

[5] Logitech Unifying Receiver Update: https://support.logi.com/hc/en-001/community/posts/360033230614-Logitech-Unifying-Receiver-Update

[6] Heise-Artikel der sich vor allem der schwierigen Update-Situation annimmt: https://www.heise.de/ct/artikel/c-t-deckt-auf-Tastaturen-und-Maeuse-von-Logitech-weitreichend-angreifbar-4464149.html

[7] Liste von Tastaturen und Mäusen, welche auf die sogenannten «MouseJack» Attacken anfällig sind: https://www.bastille.net/research/vulnerabilities/mousejack/affected-devices

Links zur verwendeten Software

https://github.com/insecurityofthings/jackit

https://github.com/BastilleResearch/mousejack

https://github.com/mame82/LOGITacker