Mailverkehr

Logitech Email vom 25. Juni (mit Bezug auf gemeldete Sicherheitslücken Wireless Input Produkten und diesbezüglichen Vortrag bei LKA NRW)

```
-------- Original-Nachricht --------
An 25. Juni 2019, 23:38, <Logitech employer, name removed> schrieb:


Hi Marcus,

I saw your presentation on github, and I wanted to request an update to
the vendor response section. Although we are rolling out a fix to POC 3,
there are still clear ways customers can protect themselves from POC 1
and 2. Here is some language we request be added:

POC #1 can be fully mitigated by not re-pairing a device to your Unifying
Receiver dongle. Or, in the rare case you must re-pair or pair a new
device to your receiver, do so in an environment where no malicious
person is within 10m/30ft.

POC #2 concerns keyboards only. Logitech Bluetooth connectivity is an
alternative that is not affected by vulnerability #2.

POC #3 will be fully mitigated by a firmware update, which we expect to
be available for download in August, 2019.

Thank you,

Kind regards,
<Logitech employer, name removed>
```

Logitech Antwort mit Gegendarstellung

```
------- Original Message -------
On Wednesday, June 26, 2019 12:57 AM, mame82 <mame82@protonmail.com> wrote:

Hi <Logitech employer, name removed>,

good to get some input. I'm going to forward these additions to BSI
(CERT-Bund), as stated I handed over the case. For the repository I ask
you to file a proper pull-request (for this exact reason I asked for
github accounts of Logitech staff).

Note on PoC 1 statement: A realistic scenario for exploitation of this
vulnerability would be a drive-by attack (attacker re-pairs device) or
a supply chain attack (again, pairing initiated by attacker) in order to
obtain valid encryption keys, which could be used for remote
eavesdropping or injection. The mitigations only apply to a
re-pairing/pairing which was initiated by a user.

I personally can't confirm, neither deny the statement on PoC 2, as I
haven't investigated the BLE HID implementation, yet. Anyways, I agree,
that if there exist similar problems in BLE stack, this could be
considered as a new issue.

Statement on PoC 3 needs some clarification. For sure you noticed that
I posted a video PoC, which showcased that encrypted presentation
clickers suffer from the exact same vulnerability. Although I stumbled
on this not earlier than two days ago, it could safely be assumed that
Logitech is aware of the fact that products not belonging to the
"Unifying" line are affected. Anyways, throughout our ongoing
conversation firmware updates for "non-Unifying" products have never
been mentioned. This is one of the reasons which lead to the decision
for hand-over of the case to German CERT: I want to assure that
customers are informed about existing issues in a proper way and that
the issue is addressed for all affected devices.

Questions touching topics like information to customers and
accessibility of firmware updates remained unanswered so far.

Will non-Unifying products which suffer from the key extraction
vulnerability (PoC 3) be patched, too?

The question on CVE request remained unanswered (although you confirmed
it has been forwarded), so I filed the requests myself.

Last but not least, I noticed that the plain injection issues for R400,
R700 and R800 (reported by other researchers) are going to be fixed
utilizing key-whitelisting. Will the same mitigation measures be applied
to other devices, like "R500" clicker or "MX Anywhere 2S" mouse?

Best regards,

Marcus
```

Erläuterung, Gegendarstellung/Relativierung

PoC 1 - Abhören des Pairings von Unifying Geräten über Funk,

Ableiten des AES link encryption keys und anschließende Entschlüsselung von Tastatur-kommunikation über Funk

Referenzdokument ist hier der an Logitech übermittelte "Report 1" (Bestandteil des bereits bekannten Github Repositories). Weiter wird der Vortrag refenrenziert, in welchem darauf hingewiesen wurde, dass die zu Grunde Liegende Lücke nicht gepatcht wird.

Darstellung Logitech:

```
POC #1 can be fully mitigated by not re-pairing a device to your Unifying
Receiver dongle. Or, in the rare case you must re-pair or pair a new
device to your receiver, do so in an environment where no malicious
person is within 10m/30ft.
```

Gegendarstellung

Eine Mitigation durch Vermeidung der Durchführung von Pairings / Re-Pairings (Verbinden eines neuen oder Neuverbinden eines existierenden Wireless Gerätes zu einem Unifying receiver) widerspricht dem Einsatzzweck der Unifying Technologie. Der überwiegende Teil der beworbenen Unifying-Produktmerkmale basiert auf der Idee (mehrere) beliebige Unifying Geräte jederzeit mit beliebigen Receivern verbinden zu können.

Siehe auch: https://www.logitech.com/de-de/product/unifying-receiver-usb

Auszüge aus Produktwerbung, welche implizit den Pairing Prozess benötigen

Verbinden Sie bis zu 6 kompatible Tastaturen und Mäuse mit einem Computer über einen einzigen Unifying-Empfänger - keine Probleme mehr mit mehreren USB-Empfängern.

Sie können diesen separaten USB-Unifying-Empfänger verwenden, um einen verloren gegangenen Empfänger zu ersetzen. Er ist kompatibel mit allen Logitech Unifying-Produkten (achten Sie auf das Unifying-Logo bei kompatiblen Produkten)

Verwenden Sie einen extra Unifying-Empfänger, um eine Easy-Switch-Maus oder Tastatur - oder beides - mit einem zweiten Computer zu verbinden.

Sicherzustellen, dass sich während eines Pairings/Re-Pairings keine "malicious Person" im näheren Umfeld befindet, sollte nicht Aufgabe des Endkunden sein. Im mindesten sollte dies als gut lesbarer Hinweis auf den Produktverpackungen vermerkt werden, denn dem Endkunden liegt diese Information überhaupt nicht vor.

Einen Abstand von "10m / 30ft" zu benennen halte ich für äußerst fragwürdig. Ich habe während meiner Untersuchungen keinerlei Reichweiten- tests durchgeführt, da hierfür keine geeignet Messausstattung / -umgebung bereitsteht. Die FCC Dokumente könnten mehr Aufschluss über theoretische Reichweiten haben. Es dürfte alledings klar sein, dass die tatsächliche Abhörreichweite stark von den örtlichen Gegebenheiten und der vom potentiellen Angreifer eingesetzten Funktechnik abhängt. Qualifizierte Aussagen müssten entlang der Prozesse gängiger Abstrahlprüfverfahren gemacht werden.

Der wohl wichtigste Aspekt: Es wird hier lediglich betrachtet, dass ein passiver Angreifer ein Geräte-Pairing über Funk mitschneidet. Es dürfte sehr unwahrscheinlich sein, dass ein solch "günstiges" Szenario in der Praxis auftritt. Viel wahrscheinlicher sind drive-by oder supply-chain Angriffe. Ein Angreifer mit physichen Zugriff auf den Unifying Receiver und ein gepairtes Gerät, kann ein (Re-)Pairing selbst initiieren, um die (neu erzeugten) AES Schlüssel zu stehlen. Diese können im Anschluss beliebig oft verwendet werden, um bspw. betroffene Tastaturen über Funk abzuhören oder über Funk Tastenanschläge zu injezieren. Der Endnutzer hat keine Möglichkeit zu erkennen, dass das Gerät neu gepairt wurde (Schlüssel kompromittiert). Ein entsprechender Angriff wäre in wenigen Sekunden durchführbar (Receiver mit Tool in pairing mode setzen, Zielgerät an und aus schalten, parallel Datenaustausch über Funk mitlesen und Schlüssel generieren).

Keine der gemachten Aussagen trifft auf ein solches Szenario zu, es fehlt hier jeglicher Technische Schutz.

PoC 2 - Injektion von verschlüsselten Tastenanschlägen über Funk, ohne

Kenntnis des AES Schlüssels und unter Umgehung der Patches/Fixes bezügl. Counter-Reuse (patches wurden als Reaktion auf die 2016 veröffentlichten "MouseJack" Schwachstellen erstellt)

Referenzdokument ist hier der an Logitech übermittelte "Report 2" (Bestandteil des bereits bekannten Github Repositories). Weiter wird der Vortrag refenrenziert, in welchem darauf hingewiesen wurde, dass die zu Grunde Liegende Lücke nicht gepatcht wird.

Darstellung Logitech:

```
POC #2 concerns keyboards only. Logitech Bluetooth connectivity is an
alternative that is not affected by vulnerability #2.
```

Gegendarstellung

Die Lücke betrifft nicht nur Tastaturen, allerdings habe ich dies erst durch weitere Untersuchungen in den letzten Tagen festgestellt.

Auch Presenter wie der Logitech R500 und Logitech Spotlight verwenden offensichtlich das exakt gleiche Kommunikationbsprotokoll wie verschlüsselte Unifying Tastaturen. Wenngleich dies kein Bestandteil des ursprünglichen Reports war, lässt sich der Angriff im Falle noch wesentlich vereinfachen.

Der Angriff fußt auf verschiedenen Annahmen und Informationleaks zu verschlüsselten Funkframes, welche von einem Angreifer erfasst werden können. Im Falle von Tastaturen lassen sich trotz Verschlüsselung das Drücken der Tasten CAPSLOCK, SCROLLOCK und NUMLOCK ableiten, da diese unverschlüsselte LED reports auf Funk nach sich ziehen (unverschlüsselte Übertragung des Tastatur LED-Status für NUM-, CAPS- und SCROLL-LED).

Ein Angreifer mit physischem Zugriff zu einer Tastatur kann die notwendigen Tasten betätigen, und automatisierte Funktechnik kann auf Basis der "erlauschten" Funk frames die schwach implementierte Verschlüsselung angreifen (known plaintext attack). Im resultat können andere Tastendrücke über Funk **BELIEBIG OFT** injeziert werden. Im veröffentlichten Proof-of-Concept Video benötigt ein Angreifer etwa 15 schnelle Tastendrücke auf die CAPS-Lock Taste (wenige Sekunden), um den Angriff auszuführen. Dieser physische Zugriff ist nur einmal nötig.

Dieses aufwendig erscheinende Verfahren zum Erlangen von "known plaintext", kann im Falle von Presentern nahezu vollständig entfallen. In den weitaus meisten Fällen, dürfte ein Nutzer welcher einen Presenter bedient die Taste zum Wechsel zur nächsten Folie betätigen. Ein Angreifer hat sogar die Möglichkeit die getätigten Eingaben per Sicht zu validieren (nächste Folie, vorherige Folie etc.). Werden die verschlüsselten Daten über Funk mitgeschnitten, kann der "known plaintext" (Taste für nächste Folie, release der Taste für nächste Folie etc.) wieder aus den verschlüsselten Daten entfernt werden und beliebige neue Tastenanschläge "aufmoduliert" werden. Diese neuen Tastenanschläge können vom Angreifer über Funk beliebig oft in den Receiver des verschlüsselten Presenters injeziert werden, zu jeder Zeit.

Der verbleibende techhnische Schutz im Falle von Presentern ist dann das vereinzelt etablierte blacklisting der Tasten (der Receiver akzeptiert jegliche Tastatureingaben, unterdrückt jedoch die Tasten A-Z). Dieser Schutz kann ebenfalls einfach umgangen werden, ein PoC-Video welches dies demonstriert wurde hier veröffentlicht: https://twitter.com/mame82/status/1143093313924452353

Weiter wird als Mitigation das Thema Bluetooth angesprochen: Keines der in den Hersteller-Reports aufgeführten Testgeräte verfügte, über Bluetooth Technologie. Die Ausnahme bilden hier tatsächlich der "R500" Presenter und die "MX Anywhere 2S" Maus, welche im Zusammenhang mit dieser Lücke ursprünglich nicht betrachtet wurden. Der Umstieg auf Bluetooth kann daher nicht als Mitigation, sondern bestenfalls als Produktwerbung betrachtet werden.

PoC 3 - Extraktion der AES Schlüssel aller gepairten Geräte aus

Unifying Receivern mit Texas Instruments SoC

Referenzdokument ist hier der an Logitech übermittelte "Report 3", welcher - wie von Logitech gewünscht - noch nicht veröffentlicht wurde.

Darstellung Logitech:

```
POC #3 will be fully mitigated by a firmware update, which we expect to
be available for download in August, 2019.
```

Gegendarstellung

Das Releasedatum des Patches wird hier erstmalig erwähnt. Zum Zeitpunkt der Übermittlung des Reports an Logitech (14. März 2019) war nicht klar, dass auch Produkte außerhalb des “Unifying” Portfolios von der Schwach- stelle betroffen sind.

Beispielsweise ist es möglich mit sehr geringen Anpassungen des Proof-of- Concept codes die Schlüssel aus dem Empfänger eines R500 Presenters zu extrahieren. Dies wiederum erlaubt Injezierung beliebiger Tastenanschläge über Funk und somit Remote Code Execution.

Gleiche PoC Video: https://twitter.com/mame82/status/1143093313924452353

Es ist daher unklar, ob alle von der Schwachstelle betroffenen Logitech Geräte für einen Patch betrachtet werden. Weiterhin ist zu keiner Zeit eine Information an die Endkunden ergangen (die derzeit Medial präsenten - und durch Logitech aufgegriffenen - Schwachstellen für die Presenter R400, R700 und R800 wurden bereits 2016 veröffentlicht).

Ob der angekündigte Patch die Schwachstelle vollumfänglich für jedes Gerät schließt, kann nur nach einer Folgeüberprüfung **aller relevanter Logitech Funk-peripherie** nach Rollout des Patches bewertet werden.

Grundsätzliche Anmerkung

Es bleibt festzuhalten, dass die Informationspolitik Richtung Kunde im vorliegendem Fall nicht optimal gestaltet ist. Wie sonst soll man erklären, dass bspw. Banken in Ihren Filialen Wireless Desktop Sets einsetzen, von denen seit 2016 bekannt ist, dass sie anfällig Remote Code Execution über Funk sind (ich erspare mir ein Tagesaktuelles Beispiel).